ALGEBRAIC NUMBER THEORY (II)

YIHANG ZHU

Contents

The **goal of this course** is the proof of global and local class field theory. The course is sequel to *Algebraic Number Theory (I)* in Spring 2025.

1. Local class field theory via cohomology

1.1. **Statements of local class field theory.** Let K be a non-archimedean local field. The following two theorems are the main theorems of local class field theory.

Theorem 1.1.1 (Local Reciprocity Law)**.** *There is a continuous homomorphism $\psi_K : K^\times \to G_K^{\mathrm{ab}}$ with dense image, called the* local Artin map*, satisfying the following conditions:*

(1) *For each finite unramified extension L/K, the composition $\psi_{L/K} : K^\times \xrightarrow{\psi_K} G_K^{\mathrm{ab}} \to \mathrm{Gal}(L/K)$ sends every uniformizer in $K^\times$ to the Frobenius element in $\mathrm{Gal}(L/K)$.*
(2) *For each finite abelian extension L/K, the composition $\psi_{L/K} : K^\times \xrightarrow{\psi_K} G_K^{\mathrm{ab}} \to \mathrm{Gal}(L/K)$ is surjective and its kernel is $\mathrm{N}_{L/K}(L^\times)$.*

Theorem 1.1.2 (Local Existence Theorem)**.** *We have an inclusion-reversing bijection*

$$\{\textit{finite abelian extensions } L/K \textit{ in } K^s\} \to \{\textit{open finite index subgroups of } K^\times\},$$

sending L to $\mathrm{N}_{L/K}(L^\times)$.

Last semester, assuming the truth of Theorem 1.1.1, we used Lubin–Tate theory to establish the following:

(1) An explicit description of K^{ab}.
(2) The map ψ_K as in Theorem 1.1.1 must be unique, and it is given by an explicit formula.
(3) An explicit proof of Theorem 1.1.2.

The first goal of this course is to prove Theorem 1.1.1, namely the existence of ψ_K. We shall use group cohomology to construct this map. It will also follow from our construction that ψ_K satisfies *norm and transfer functoriality*, as recalled below:

Theorem 1.1.3 (Norm and transfer functoriality)**.** *Let L/K be a finite separable extension. Then we have a commutative diagram*

$$\begin{array}{ccc} L^\times & \xrightarrow{\psi_L} & G_L^{\mathrm{ab}} \\ {\scriptstyle \mathrm{N}_{L/K}}\downarrow & & \downarrow{\scriptstyle i} \\ K^\times & \xrightarrow{\psi_K} & G_K^{\mathrm{ab}} \end{array}$$

where i is induced by the inclusion $G_L \hookrightarrow G_K$. We have a commutative diagram

$$\begin{array}{ccc} L^\times & \xrightarrow{\psi_L} & G_L^{\mathrm{ab}} \\ \uparrow & & \uparrow V \\ K^\times & \xrightarrow{\psi_K} & G_K^{\mathrm{ab}} \end{array}$$

where V is the transfer map.

1.2. **The idea of using group cohomology.** For any group G and any G-module A (abelian group with G-action), we have the cohomology groups $\mathbf{H}^i(G, A), i \geq 0$, which are abelian groups. If G is finite, then we have the Tate cohomology groups $\widehat{\mathbf{H}}^i(G, A), i \in \mathbb{Z}$. In order to construct the Artin map ψ_K, for each finite abelian extension L/K we need to construct the isomorphism

$$\psi_{L/K}^{-1} : \mathrm{Gal}(L/K) \xrightarrow{\sim} K^\times/\mathrm{N}_{L/K}(L^\times).$$

The two sides have group cohomology interpretations: The left hand side is $\widehat{\mathbf{H}}^{-2}(\mathrm{Gal}(L/K), \mathbb{Z})$ where $\mathbb{Z}$ has the trivial $\mathrm{Gal}(L/K)$-action (more generally, for any finite group G, $\widehat{\mathbf{H}}^{-2}(G, \mathbb{Z})$ is the abelianization of G), and the right hand side is $\widehat{\mathbf{H}}^0(\mathrm{Gal}(L/K), L^\times)$. In general, we have the cup product

$$\cup : \widehat{\mathbf{H}}^i(G, A) \otimes \widehat{\mathbf{H}}^j(G, B) \to \widehat{\mathbf{H}}^{i+j}(G, A \otimes B).$$

Moreover, there is a distinguished element, called the fundamental class,

$$c \in \widehat{\mathbf{H}}^2(\mathrm{Gal}(L/K), L^\times).$$

The desired map $\psi_{L/K}^{-1}$ will be given by cupping with c:

$$\psi_{L/K}^{-1}(x) := x \cup c.$$

1.3. **The category of G-modules.** Let G be a group. By a *G-module*, we mean an abelian group equipped with a left G-action via group automorphisms. Let $\mathbb{Z}[G]$ be the group algebra of G over $\mathbb{Z}$. This is the ring consisting of formal finite linear combinations $\sum_{i=1}^n a_i[g_i]$, with $a_i \in \mathbb{Z}$ and $g_i \in G$, and multiplication is given by

$$(\sum_i a_i[g_i])(\sum_j b_j[h_j]) = \sum_{i,j} a_i b_j [g_i h_j].$$

Then a G-module is the same as a left $\mathbb{Z}[G]$-module. Morphisms between G-modules are group homomorphisms which are G-equivariant. (We shall also call these morphisms *G-homomorphisms*.) The category of G-modules is abelian.

If X, Y are G-modules, we write $\mathrm{Hom}(X, Y)$ for the group of homomorphisms $X \to Y$, and write $\mathrm{Hom}_{\mathbb{Z}[G]}(X, Y) = \mathrm{Hom}_G(X, Y)$ for the group of G-homomorphisms $X \to Y$. Note that $\mathrm{Hom}(X, Y)$ is naturally a G-module, with the G-action defined by $(gf)(x) = g(f(g^{-1}x)), \forall g \in G, f \in \mathrm{Hom}(X, Y), x \in X$. We have $\mathrm{Hom}_G(X, Y) = \mathrm{Hom}(X, Y)^G$.

Similarly, if X, Y are G-modules, then $X \otimes_{\mathbb{Z}} Y$ is naturally a G-module, where the G-action is defined by $g(x \otimes y) = gx \otimes gy$.

Let H be a subgroup of G. We have two functors from H-modules to G-modules, called *induction* and *coinduction*, defined by

$$\mathrm{Ind}_H^G(X) = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} X,$$
$$\mathrm{coInd}_H^G(X) = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], X).$$

In the first definition, $\mathbb{Z}[G]$ is viewed as a right $\mathbb{Z}[H]$-module by right multiplication of H on G, and the G-action on $\mathrm{Ind}_H^G(X)$ is induced by the left multiplication of G on $\mathbb{Z}[G]$. In the second definition, $\mathbb{Z}[G]$ is viewed as a left $\mathbb{Z}[H]$-module by left multiplication of H on G, and the G-action on $\mathrm{coInd}_H^G(X)$ is induced by right multiplication of G on $\mathbb{Z}[G]$, i.e., for $g_0 \in G$ and $f \in \mathrm{coInd}_H^G(X)$, we define

$$(g_0 f)(\sum_i a_i[g_i]) := f(\sum_i a_i[g_i g_0]), \quad \forall \sum_i a_i[g_i] \in \mathbb{Z}[G].$$

We can make these definitions more concrete. For induction, we can fix coset representatives for G/H, so that $G = \bigsqcup_{i\in I} g_i H$. Then the right $\mathbb{Z}[H]$-module $\mathbb{Z}[G]$ is free with basis $\{[g_i]\}_{i\in I}$. Therefore

$$\mathrm{Ind}_H^G X \cong \bigoplus_{i\in I} [g_i] \otimes X,$$

and each $[g_i] \otimes X$ is isomorphic to X as an abelian group. We can interpret elements of this direct sum as finitely supported functions $\{g_i\}_{i\in I} \to X$, i.e., if ϕ is such a function, then the corresponding element in the direct sum is $\sum_i [g_i] \otimes \phi(g_i)$. From this point of view, one can write down an explicit formula for the G-action on $\mathrm{Ind}_H^G X$ as follows: Let $g \in G$. For each $i \in I$, there exists $s(i) \in I$ and $h_i \in H$ such that $gg_i = g_{s(i)}h_i$. Clearly $s : I \to I$ is a bijection. We have

$$g(\sum_i [g_i] \otimes \phi(g_i)) = \sum_i [gg_i] \otimes \phi(g_i) = \sum_i [g_{s(i)}] \otimes h_i \phi(g_i).$$

Hence the new function $g \cdot \phi : \{g_i\} \to X$ sends g_i to $h_{s^{-1}(i)}\phi(g_{s^{-1}(i)})$.

Similarly, we can fix coset representatives for $H\backslash G$, so that $G = \bigsqcup_{i\in I} Hg_i$. Then $\mathrm{coInd}_H^G X$ is the space of (all) functions $\{g_i\} \to X$, and one can also write down explicitly the G-action on it.

Clearly Ind_H^G and coInd_H^G are additive functors from the category of H-modules to the category of G-modules. The concrete descriptions above immediately imply the following:

Lemma 1.3.1. *The functors Ind_H^G and coInd_H^G are exact, i.e., they send exact sequences of H-modules to exact sequences of G-modules.*

Exercise 1.3.2. If H is of finite index in G, then the functors Ind_H^G and coInd_H^G are naturally isomorphic. (Hint: Use $g \mapsto g^{-1}$ to relate G/H and $H\backslash G$.)

Let X be a G-module. Write X_0 for X viewed as an H-module. Then we have an injective G-homomorphism

$$X \longrightarrow \mathrm{coInd}_H^G(X_0), \quad x \longmapsto (\sum_i a_i[g_i] \mapsto \sum_i a_i g_i(x)).$$

(It is injective because the image of x sends $[1] \in \mathbb{Z}[G]$ to x.) Also we have a surjective G-homomorphism

$$\mathrm{Ind}_H^G(X_0) \longrightarrow X, \quad (\sum_i a_i[g_i]) \otimes x \longmapsto \sum_i a_i g_i(x).$$

Exercise 1.3.3. Check the following two versions of Frobenius reciprocity: Let H be a subgroup of G. For any G-module X and H-module A, we have a natural isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[H]}(X_0, A) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}[G]}(X, \mathrm{coInd}_H^G A)$$

sending $f : X_0 \to A$ to the composite map

$$X \to \mathrm{coInd}_H^G X_0 \xrightarrow{\mathrm{coInd}_H^G(f)} \mathrm{coInd}_H^G A.$$

Also we have an isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[H]}(A, X_0) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathrm{Ind}_H^G A, X)$$

sending $f : A \to X_0$ to the composite map

$$\mathrm{Ind}_H^G A \xrightarrow{\mathrm{Ind}_H^G(f)} \mathrm{Ind}_H^G X_0 \to X.$$

Let Res_H^G be the functor from G-modules to H-modules sending a G-module to itself viewed as an H-module. Then the above exercise shows that Res_H^G has left adjoint Ind_H^G and right adjoint coInd_H^G.

Recall that in an abelian category $\mathcal{A}$, an object I is called *injective* (resp. *projective*) if the functor $\mathrm{Hom}_{\mathcal{A}}(\cdot, I)$ (resp. $\mathrm{Hom}_{\mathcal{A}}(I, \cdot)$) from $\mathcal{A}$ to the category of abelian groups is exact. The category is said to have enough injectives, if for every object A there exists a monomorphism $A \to I$ where I is injective. The category is said to have enough projectives, if for every object A there exists an epimorphism $P \to A$ where P is projective.

If $\mathcal{A}$ has enough injectives, then every object A admits an *injective resolution*, namely an exact complex

$$0 \to A \to I^0 \to I^1 \to \cdots$$

where each I^i is injective. (To construct it, first find a monomorphism $A \to I^0$. Then by induction, if we already have $A \to I^0 \to \cdots \to I^n$, find a monomorphism $\mathrm{Cok}(I^{n-1} \to I^n) \hookrightarrow I^{n+1}$ with I^{n+1} injective.) Similarly, if $\mathcal{A}$ has enough projectives, then every object A admits a projective resolution

$$\cdots \to P_1 \to P_0 \to A \to 0$$

where each P_i is projective.

Exercise 1.3.4. In the category of abelian groups, an abelian group A is injective if and only if it is divisible, namely for every $a \in A$ and $n \in \mathbb{Z}_{>0}$, there exists $b \in A$ such that $a = nb$. Every free abelian group is projective. Then show that the category of abelian groups has enough projectives and enough injectives. (Hint: for the latter, show that for every abelian group A there is an injection $A \to \prod_{\chi \in \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})} \mathbb{Q}/\mathbb{Z}$.)

Lemma 1.3.5. *If A is an injective abelian group, then $\mathrm{coInd}_1^G A$ is an injective G-module. If A is a projective abelian group, then $\mathrm{Ind}_1^G A$ is a projective G-module.*

Proof. This follows easily from Frobenius reciprocity. □

Corollary 1.3.6. *The category of G-modules has enough injectives and enough projectives.*

Proof. Let X be a G-module, and X_0 the underlying abelian group of X. The category of abelian groups have enough injective objects, so we can find an injective homomorphism $X_0 \to I_0$ where I_0 is an injective abelian group. Since coInd_1^G is exact, we have injective G-homomorphisms $X \to \mathrm{coInd}_1^G X_0 \to \mathrm{coInd}_1^G I_0$. By Lemma 1.3.5, $\mathrm{coInd}_1^G I_0$ is an injective G-module.

The proof of enough projective objects is similar, using that the category of abelian groups has enough projectives and using the surjection $\mathrm{Ind}_1^G X_0 \to X$. □

By the above corollary, for any left exact additive functor $\mathcal{F}$ from G-modules to an abelian category, we have the right derived functors $R^i\mathcal{F}, i \geq 0$. Similarly, for any right exact additive functor $\mathcal{G}$ from G-modules to an abelian category, we have the left derived functors $L_i\mathcal{G}, i \geq 0$.

1.4. **Recall of derived functors.** (See [Wei94, §2] for details.)

Definition 1.4.1. Let $\mathcal{A}, \mathcal{B}$ be abelian categories.

(1) A *cohomological δ-functor* is a collection $(\mathcal{F}^i, \delta)$, where $\mathcal{F}^i : \mathcal{A} \to \mathcal{B}$ are additive functors for $i \geq 0$, and δ is the datum of a morphism $\mathcal{F}^i(Z) \to \mathcal{F}^{i+1}(X)$ for each i and each short exact sequence $0 \to X \to Y \to Z \to 0$ in $\mathcal{A}$. These should satisfy:
   (a) For every short exact sequence $0 \to X \to Y \to Z \to 0$ in $\mathcal{A}$, we have a long exact sequence

$$0 \to \mathcal{F}^0(X) \to \mathcal{F}^0(Y) \to \mathcal{F}^0(Z) \xrightarrow{\delta} \mathcal{F}^1(X) \to \mathcal{F}^1(Y) \to \mathcal{F}^1(Z) \xrightarrow{\delta} \mathcal{F}^2(X) \to \cdots$$

   (b) If we have a commutative diagram with exact rows in $\mathcal{A}$:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & X' & \longrightarrow & Y' & \longrightarrow & Z' & \longrightarrow & 0 \end{array}$$

   then for each $i \geq 0$ the following diagram commutes:

$$\begin{array}{ccc} \mathcal{F}^i(Z) & \xrightarrow{\delta} & \mathcal{F}^{i+1}(X) \\ \downarrow & & \downarrow \\ \mathcal{F}^i(Z') & \xrightarrow{\delta} & \mathcal{F}^{i+1}(X') \end{array}$$

(2) A *homological δ-functor* is a collection $(\mathcal{F}_i, \delta)$, where $\mathcal{F}_i : \mathcal{A} \to \mathcal{B}$ are additive functors for $i \geq 0$, and δ is the datum of a morphism $\mathcal{F}_{i+1}(Z) \to \mathcal{F}_i(X)$ for each i and each short exact sequence $0 \to X \to Y \to Z \to 0$ in $\mathcal{A}$. These should satisfy:
   (a) For every short exact sequence $0 \to X \to Y \to Z \to 0$ in $\mathcal{A}$, we have a long exact sequence

$$\cdots \to \mathcal{F}_2(Z) \xrightarrow{\delta} \mathcal{F}_1(X) \to \mathcal{F}_1(Y) \to \mathcal{F}_1(Z) \xrightarrow{\delta} \mathcal{F}_0(X) \to \mathcal{F}_0(Y) \to \mathcal{F}_0(Z) \to 0.$$

   (b) The analogue of (1)(b).

There is an obvious notion of morphisms between δ-functors. For instance, a morphism between cohomological δ-functors $(\mathcal{F}^i, \delta) \to (\mathcal{F}'^{,i}, \delta')$ is a collection of natural transformations $\mathcal{F}^i \to \mathcal{F}'^{,i}$ which are compatible with δ in the obvious sense.

We now discuss right derived functors. Fix $\mathcal{F} : \mathcal{A} \to \mathcal{B}$ a left exact additive functor between abelian categories.[1] Assume that $\mathcal{A}$ has enough injectives.

Theorem 1.4.2. *There is a unique (up to isomorphism) cohomological δ-functor $(R^i\mathcal{F}, \delta)$, called the right derived functors of $\mathcal{F}$, satisfying the following conditions:*

(1) $R^0\mathcal{F} \cong \mathcal{F}$.

[1] An additive functor $\mathcal{F} : \mathcal{A} \to \mathcal{B}$ between abelian categories is called *left (resp. right) exact*, if for any short exact sequence $0 \to X \to Y \to Z \to 0$ in $\mathcal{A}$, the sequence $0 \to \mathcal{F}(X) \to \mathcal{F}(Y) \to \mathcal{F}(Z)$ (resp. $\mathcal{F}(X) \to \mathcal{F}(Y) \to \mathcal{F}(Z) \to 0$) is exact.

(2) *If $(\mathcal{G}^i, \delta')$ is another cohomological δ-functor, then every natural transformation $R^0\mathcal{F} \to \mathcal{G}^0$ extends uniquely to a morphism of δ-functors $(R^i\mathcal{F}, \delta) \to (\mathcal{G}^i, \delta')$*

Fact 1.4.3. *One can compute $R^i\mathcal{F}$ using injective resolution. For $X \in \mathcal{A}$, we find an injective resolution $0 \to X \to I^0 \to I^1 \to \cdots$. Then $R^i\mathcal{F}(X) \in \mathcal{B}$ is the i-th cohomology object of the complex $\mathcal{F}(I^0) \to \mathcal{F}(I^1) \to \cdots$ in $\mathcal{B}$. (We shall write the resolution as $0 \to X \to I^\bullet$, and write the above complex as $\mathcal{F}(I^\bullet)$.) In particular, if X is injective, then $R^i\mathcal{F}(X) = 0$ for all $i \geq 1$.*

Definition 1.4.4. A cohomological δ-functor $(\mathcal{F}^i, \delta)$ is called *effaceable*, if for every $X \in \mathcal{A}$ there exists a monomorphism $X \to X'$ such that $\mathcal{F}^i(X') = 0$ for all $i \geq 1$.

By our assumption that $\mathcal{A}$ has enough injectives and by the fact that $R^i\mathcal{F}(X) = 0$ for X injective, we know that the family of right derived functors $R^i\mathcal{F}$ of $\mathcal{F}$ is effaceable. We have the following criterion for recognizing derived functors.

Fact 1.4.5. *The family of right derived functors of $\mathcal{F}$ is the unique (up to isomorphism) effaceable cohomological δ-functor whose 0-th member is $\mathcal{F}$. More precisely, if $(\mathcal{G}^i, \delta')$ is an effaceable δ-functor, then any isomorphism $R^0\mathcal{F} \xrightarrow{\sim} \mathcal{G}^0$ extends to an isomorphism of δ-functors $(R^i\mathcal{F}, \delta) \xrightarrow{\sim} (\mathcal{G}^i, \delta')$.*

We now discuss left derived functors, which is completely analogous. Fix $\mathcal{F} : \mathcal{A} \to \mathcal{B}$ a right exact additive functor between abelian categories. Assume that $\mathcal{A}$ has enough projectives.

Theorem 1.4.6. *There is a unique (up to isomorphism) homological δ-functor $(L_i\mathcal{F}, \delta)$, called the left derived functors of $\mathcal{F}$, satisfying the following conditions:*

(1) *$L_0\mathcal{F} \cong \mathcal{F}$.*
(2) *If $(\mathcal{G}_i, \delta')$ is another homological δ-functor, then every natural transformation $\mathcal{G}_0 \to L_0\mathcal{F}$ extends uniquely to a morphism of δ-functors $(\mathcal{G}_i, \delta') \to (L_i\mathcal{F}, \delta)$.*

Fact 1.4.7. *One can compute $L_i\mathcal{F}$ using projective resolution. For $X \in \mathcal{A}$, we find an projective resolution $\cdots \to P_1 \to P_0 \to X \to 0$. Then $L^i\mathcal{F}(X) \in \mathcal{B}$ is the i-th cohomology object of the complex $\cdots \to \mathcal{F}(P_1) \to \mathcal{F}(P_0)$ in $\mathcal{B}$. In particular, if X is projective, then $L_i\mathcal{F}(X) = 0$ for all $i \geq 1$.*

Definition 1.4.8. A homological δ-functor $(\mathcal{F}_i, \delta)$ is called *effaceable*, if for every $X \in \mathcal{A}$ there exists an epimorphism $X' \to X$ such that $\mathcal{F}_i(X') = 0$ for all $i \geq 1$.

Fact 1.4.9. *The family of left derived functors of $\mathcal{F}$ is the unique (up to isomorphism) effaceable homological δ-functor whose 0-th member is $\mathcal{F}$.*

Now suppose that $\mathcal{F} : A \to B$ is a right exact additive functor between abelian categories, and that $\mathcal{A}$ has enough projectives. Then the left derived functors $L_i\mathcal{F}$ $(i \geq 0)$ are defined. These turn short exact sequences $0 \to X \to Y \to Z \to 0$ to long exact sequences of the form

$$\cdots \to L_2\mathcal{F}(Z) \to L_1\mathcal{F}(X) \to L_1\mathcal{F}(Y) \to L_1\mathcal{F}(Z) \to L_0\mathcal{F}(X) \to L_0\mathcal{F}(Y) \to L_0\mathcal{F}(Z) \to 0,$$

and are similarly characterized by $L_0\mathcal{F} = \mathcal{F}$ and a universal property as before. For each X in $\mathcal{A}$, take a projective resolution

$$\cdots \to P_1 \to P_0 \to X \to 0.$$

Then $L_i\mathcal{F}(X)$ is the i-th homology of the complex $\mathcal{F}(P_\bullet)$.

1.5. **Definition of group (co)homology.** Given any G-module X, we define the G-invariants

$$X^G = \{x \in X \mid gx = x, \forall g \in G\}$$

and the G-coinvariants

$$X_G = X/\langle gx - x \mid g \in G, x \in X\rangle.$$

Then $X \mapsto X^G$ and $X \mapsto X_G$ are functors from G-modules to abelian groups. Note that they are left exact and right exact respectively.

Definition 1.5.1. For $i \geq 0$, we define $\mathbf{H}^i(G, \cdot)$ to be the i-th right derived functor of the left exact functor $X \mapsto X^G$ from G-modules to abelian groups. We define $\mathbf{H}_i(G, \cdot)$ to be the i-th left derived functor of the right exact functor $X \mapsto X_G$ from G-modules to abelian groups.

Example 1.5.2. By definition we have $\mathbf{H}^0(G, X) = X^G$ and $\mathbf{H}_0(G, X) = X_G$.

Example 1.5.3. Let G be the trivial group. Then $\mathbf{H}^i(G, X) = \mathbf{H}_i(G, X) = 0$ for $i > 0$.

Exercise 1.5.4. Let $(M_j)_{j\in J}$ be a family of G-modules. Then $\mathbf{H}^i(G, \prod_j M_j) \cong \prod_j \mathbf{H}^i(G, M_j)$.

1.6. **Alternative definition using free resolution of $\mathbb{Z}$.** Note that the functor $X \mapsto X^G$ from G-modules to abelian groups can be alternatively regarded as the functor $X \mapsto \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, X)$, where $\mathbb{Z}$ is equipped with the trivial G-action.

Fact 1.6.1. *Let $\mathcal{A}$ be an abelian category with enough injectives. Fix $A \in \mathcal{A}$, and let $\mathrm{Ext}^i(A, \cdot)$ be the right derived functors of the functor $\mathrm{Hom}(A, \cdot) : \mathcal{A} \to \{$abelian groups$\}$. Suppose A has a projective resolution $P_\bullet \to A \to 0$. Then $\mathrm{Ext}^i(A, X)$ can be computed as the i-th cohomology of $\mathrm{Hom}(P_\bullet, X)$.*

Thus $\mathbf{H}^i(G, X) = \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, X)$. If we take a projective resolution

$$\cdots \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

of $\mathbb{Z}$ in the category of G-modules (which exists), then $\mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, X)$ can be computed as the i-th cohomology of

$$\mathrm{Hom}_{\mathbb{Z}[G]}(P_0, X) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, X) \to \cdots.$$

This gives an alternative, and in fact more practical, way of computing $\mathbf{H}^i(G, X)$. Note that we can fix the resolution $P_\bullet$ once and for all, independently of X.

We will soon exhibit a *free resolution* $P_\bullet \to \mathbb{Z} \to 0$, i.e., each P_i is a direct sum of copies of $\mathbb{Z}[G]$. Note that any free $\mathbb{Z}[G]$-module is projective. With such a resolution we can also compute $\mathbf{H}_i(G, \cdot)$. We view the left G-module P_i also as a right G-module by defining $p \cdot g$ to be $g^{-1} \cdot p$, for $p \in P_i, g \in G$. Then $P_\bullet \to \mathbb{Z} \to 0$ is also a free resolution in the category of right $\mathbb{Z}[G]$-modules.

Lemma 1.6.2. *Each $\mathbf{H}_i(G, X)$ is the i-th homology of*

$$\cdots \to P_1 \otimes_{\mathbb{Z}[G]} X \to P_0 \otimes_{\mathbb{Z}[G]} X.$$

Proof. Let $\mathcal{G}_i$ be the functor sending X to the i-th homology of the complex as in the lemma. We first show that the $(\mathcal{G}_i)$ can be naturally enhanced to a homological δ-functor. In other words, we need to show that for any short exact sequence $0 \to X \to Y \to Z \to 0$ of G-modules we have functorially a long exact sequence

$$\cdots \to \mathcal{G}_1(Z) \to \mathcal{G}_0(X) \to \mathcal{G}_0(Y) \to \mathcal{G}_0(Z) \to 0. \tag{1.1}$$

For this, observe that $0 \to P_i \otimes_{\mathbb{Z}[G]} X \to P_i \otimes_{\mathbb{Z}[G]} Y \to P_i \otimes_{\mathbb{Z}[G]} Z \to 0$ is exact for all i, since $P_i \otimes_{\mathbb{Z}[G]} R$ is just a direct sum of copies of R for any G-module R. Then we would obtain a short exact sequence of complexes $0 \to P_\bullet \otimes_{\mathbb{Z}[G]} X \to P_\bullet \otimes_{\mathbb{Z}[G]} Y \to P_\bullet \otimes_{\mathbb{Z}[G]} Z \to 0$, from which we obtain a long exact sequence of the homology groups of the complexes, i.e. a long exact sequence (1.1).

We have $\mathcal{G}_0(X) \cong (P_0/P_1) \otimes_{\mathbb{Z}[G]} X \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} X \cong \mathbf{H}_0(G, X)$. Thus by Fact 1.4.9, it suffices to check that for every G-module X there is an epimorphism $X' \to X$ such that $\mathcal{G}_i(X') = 0$ for all $i > 0$. We take $X' = \mathrm{Ind}_1^G X = \mathbb{Z}[G] \otimes_{\mathbb{Z}} X$. We need to show that the complex

$$\cdots \to P_1 \otimes_{\mathbb{Z}[G]} X' \to P_0 \otimes_{\mathbb{Z}[G]} X'$$

is exact. But each term is $P_i \otimes_{\mathbb{Z}} X$. The P_i's are free abelian groups, so the homology of the above complex computes $\mathrm{Tor}_i(\mathbb{Z}, X)$, where $\mathrm{Tor}_i(\cdot, X)$ are the left derived functors of $(\cdot) \otimes_{\mathbb{Z}} X$ from abelian groups to abelian groups. But $\mathbb{Z}$ is projective as an abelian group, so $\mathrm{Tor}_i(\mathbb{Z}, X) = 0$ for $i \geq 1$. □

Remark 1.6.3. The proof of Fact 1.6.1 is similar and easier. The functors sending X to the cohomology groups of $\mathrm{Hom}(P_\bullet, X)$ form a cohomological δ-functor. The zero-th cohomology is $\ker(\mathrm{Hom}(P_0, X) \to \mathrm{Hom}(P_1, X)) \cong \mathrm{Hom}(P_0/P_1, X) \cong \mathrm{Hom}(A, X)$. To show that this δ-functor is effaceable, for every $X \in \mathcal{A}$ we take a monomorphism $X \to X'$ with X' injective, and we only need to show that $\mathrm{Hom}(P_\bullet, X')$ is exact. But this follows directly from the injectivity of X' (so $\mathrm{Hom}(\cdot, X')$ turns arbitrary, not just short, exact sequences into exact sequences).

Proposition 1.6.4 (Shapiro's Lemma)**.** *Let H be a subgroup of G. For each H-module X, there are natural isomorphisms*

$$\mathbf{H}^i(G, \mathrm{coInd}_H^G X) \cong \mathbf{H}^i(H, X)$$

and

$$\mathbf{H}_i(G, \mathrm{Ind}_H^G X) \cong \mathbf{H}_i(H, X)$$

for $i \geq 0$.

Proof. Fix a free resolution $P_\bullet \to \mathbb{Z} \to 0$ in the category of G-modules. Then $\mathbf{H}^i(G, \mathrm{coInd}_H^G X)$ is the i-th cohomology of $\mathrm{Hom}_{\mathbb{Z}[G]}(P_\bullet, \mathrm{coInd}^G X)$, which is the same as $\mathrm{Hom}_{\mathbb{Z}[H]}(P_\bullet, X)$ by Frobenius reciprocity. Note that $P_\bullet \to \mathbb{Z} \to 0$ is also a free resolution in the category of $\mathbb{Z}[H]$-modules. (Everything free over $\mathbb{Z}[G]$ is also free over $\mathbb{Z}[H]$.) Hence the cohomology of $\mathrm{Hom}_{\mathbb{Z}[H]}(P_\bullet, X)$ is $\mathbf{H}^i(H, X)$.

The statement about homology is proved similarly. □

Definition 1.6.5. A G-module is called *induced* (resp. *coinduced*), if it is of the form $\mathrm{Ind}_1^G A$ (resp. $\mathrm{coInd}_1^G A$) for an abelian group A. A G-module is called *relatively injective* (resp. *relatively projective*), if it is a direct summand of a coinduced (resp. induced) G-module.

Corollary 1.6.6. *Let X be a relatively injective G-module. Then $\mathbf{H}^i(G, X) = 0$ for $i \geq 1$. Let Y be a relatively projective G-module, then $\mathbf{H}_i(G, Y) = 0$ for $i \geq 1$.*

Proof. This follows from Shapiro's Lemma and Example 1.5.3. □

1.7. **The standard free resolution of $\mathbb{Z}$.** We now describe an explicit choice of a free resolution $P_\bullet \to \mathbb{Z} \to 0$ in the category of G-modules. Let $P_i = \mathbb{Z}[G^{i+1}]$, with G-action given by

$$g \cdot [g_0, g_1, \dots, g_i] = [gg_0, \dots, gg_i], \quad \forall g \in G, (g_0, \dots, g_i) \in G^{i+1}.$$

Note that P_i is indeed a free $\mathbb{Z}[G]$-module, with a $\mathbb{Z}[G]$-basis

$$\{[1, g_1, \dots, g_i] \mid g_1, \dots, g_i \in G\}.$$

Define the differential $d_i : P_i \to P_{i-1}$ by

$$d_i[g_0, \dots, g_i] := \sum_{0 \le j \le i} (-1)^j [g_0, \dots, \widehat{g_j}, \dots, g_i], \quad \forall (g_0, \dots, g_i) \in G^{i+1}.$$

Here hat means ommision. Define $\epsilon : P_0 \to \mathbb{Z}$ by $\epsilon[g_0] = 1, \forall g_0 \in G$. (This is called the augmentation map.)

Proposition 1.7.1. *The following is an exact complex in the category of G-modules:*

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} \mathbb{Z} \to 0.$$

In particular, it is a free resolution of $\mathbb{Z}$. We call it the standard free resolution.

Proof. It is routine to check that this is a complex (i.e., the composition of any two consecutive maps is zero). The exactness at P_0 is also easy. We check exactness at P_i for $i \ge 1$. For every $q \ge 0$ define $h_q : P_q \to P_{q+1}$ by $[g_0, \dots, g_q] \mapsto [1, g_0, \dots, g_q]$. Then for $x = [g_0, \dots, g_i] \in P_i$,

$$(d_{i+1} \circ h_i)x = x + \sum_{j=1}^{i+1} (-1)^j [1, g_0, \dots, \hat{g}_{j-1}, \dots, g_i] = x - (h_{i-1} \circ d_i)x.$$

Thus by linearity we have

$$(d_{i+1} \circ h_i)x = x - (h_{i-1} \circ d_i)x$$

for all $x \in P_i$. If x lies in the kernel of d_i, then the above shows that $x = d_{i+1}(h_i(x))$. □

Remark 1.7.2. The same proof shows that for any finite set S, we have an analogous exact complex of abelian groups $P_\bullet \to \mathbb{Z} \to 0$ where $P_i = \mathbb{Z}[S^{i+1}]$. This complex is nothing but the augmented ordered chain complex (see below) of the $|S| - 1$ dimensional simplex Δ^S with vertex set S. Thus the homology of this complex computes the reduced homology of Δ^S, and this is indeed zero since Δ^S is contractible.

1.8. **Digression into algebraic topology.** (See [Bro94, §§I.4, II.4, III.1] for details.) Let G be a group. As Remark 1.7.2 suggests, there is a close relation between free resolutions of $\mathbb{Z}$ in the category of G-modules and algebraic topology. We consider the following two settings:

CW setting. Let X be a CW complex with a G-action such that G freely permutes the cells. Let $P_\bullet \to \mathbb{Z} \to 0$ be the usual augmented cellular chain complex for X, where P_i is the free abelian group generated by the i-dimensional cells. Since G freely permutes the i-dimensional cells, P_i is a free $\mathbb{Z}[G]$-module. Moreover, $P_\bullet \to \mathbb{Z} \to 0$ is a complex in the category of G-modules. The homology of this complex computes the reduced homology of X. Hence we obtain a free resolution of $\mathbb{Z}$ if X is contractible.

Simplicial setting. Let X be a simplicial complex with a G-action such that G freely permutes the vertices. Let $P_\bullet \to \mathbb{Z} \to 0$ be the augmented ordered chain complex, where P_i is the free abelian group generated by ordered $(i+1)$-tuples of vertices, and $d : P_{i+1} \to$

$P_i, [v_0, \dots, v_{i+1}] \mapsto \sum_j (-1)^j [v_0, \dots, \hat{v}_j, \dots, v_{i+1}]$. Since G freely permutes the vertices, P_i is a free $\mathbb{Z}[G]$-module. Moreover, $P_\bullet \to \mathbb{Z} \to 0$ is a complex in the category of G-modules. The homology of this complex computes the reduced homology of X. Hence we obtain a free resolution of $\mathbb{Z}$ if X is contractible.

How do we construct such a contractible X systematically? Let Y be either a connected CW complex or a connected simplicial complex such that $\pi_1(Y, y) = G$ for some base point $y \in Y$. Assume the universal cover X of Y is contractible. A space Y satisfying these conditions is called $K(G, 1)$ or an *Eilenberg–MacLane space*. For such Y, the universal cover X with the natural G-action satisfies our conditions before, in either of the two settings. Thus we obtain a free resolution of $\mathbb{Z}$ in the category of G-modules.

From this discussion we also obtain a topological interpretation of $\mathbf{H}^i(G, \mathbb{Z})$ and $\mathbf{H}_i(G, Z)$. Recall that $\mathbf{H}_i(G, \mathbb{Z})$ is the i-th homology of the complex $(P_\bullet \otimes_{\mathbb{Z}[G]} \mathbb{Z}) = (P_\bullet)_G$. If $P_\bullet$ is constructed from the universal cover $X \to Y$ as above, then it is easy to see that the complex $(P_\bullet)_G$ is nothing but the cellular chain complex (resp. ordered chain complex) for Y in the CW setting (resp. simplicial setting). Therefore

$$\mathbf{H}_i(G, \mathbb{Z}) \cong \mathbf{H}_i(Y, \mathbb{Z}).$$

Similarly,

$$\mathbf{H}^i(G, \mathbb{Z}) \cong \mathbf{H}^i(Y, \mathbb{Z}).$$

1.9. **Computing cohomology.** Let X is a G-module. Recall that $\mathbf{H}^i(G, X)$ is the i-th cohomology of $\mathrm{Hom}_{\mathbb{Z}[G]}(P_\bullet, X)$. Now $\mathrm{Hom}_{\mathbb{Z}[G]}(P_i, X)$ is identified with abelian group $\tilde{C}^i(G, X)$ consisting of functions $f : G^{i+1} \to X$ satisfying the *homogeneous condition*

$$f(gg_0, \dots, gg_i) = g \cdot f(g_0, \dots, g_i).$$

Such functions are called *homogeneous i-cochains*. The differential $\tilde{d} : \tilde{C}^i(G, X) \to \tilde{C}^{i+1}(G, X)$ induced by $d : P_{i+1} \to P_i$ is given by

$$(\tilde{d}f)(g_0, \dots g_{i+1}) = \sum_{j=0}^{i} (-1)^j f(g_0, \dots, \widehat{g_j}, \dots, g_i)$$

We would like to dehomogenize $\tilde{C}^i(G, X)$. Let $C^i(G, X)$ be the abelian group of all maps $G^i \to X$. We have an isomorphism

$$\tilde{C}^i(G, X) \xrightarrow{\sim} C^i(G, X), \quad f \mapsto \big((g_1, \dots, g_i) \mapsto f(1, g_1, g_1 g_2, \dots, g_1 \cdots g_i)\big).$$

The induced differential $d : C^i(G, X) \to C^{i+1}(G, X)$ is given by

$$(df)(g_1, \dots, g_{i+1}) = g_1 f(g_2, \dots, g_{i+1}) + \sum_{j=1}^{i} (-1)^j f(g_1, \dots, g_j g_{j+1}, \dots, g_{i+1}) + (-1)^{i+1} f(g_1, \dots, g_i).$$

The kernel and image of $d : C^i(G, X) \to C^{i+1}(G, X)$ are denoted by $Z^i(G, X)$ and $B^{i+1}(G, X)$, and their elements are called i-cocycles and $i+1$-coboundaries (for $i \geq 0$). We have $\mathbf{H}^0(G, X) = Z^0(G, X)$ and

$$\mathbf{H}^i(G, X) = Z^i(G, X)/B^i(G, X), \quad i \geq 1.$$

Example 1.9.1. The differential $d^0 : C^0(G, X) = X \to C^1(G, X)$ sends $x \in X$ to the function $G \to X, g \mapsto gx - x$. Its kernel is indeed $\mathbf{H}^0(G, X) = X^G$.

Example 1.9.2. The differential $d^1 : C^1(G,X) \to C^2(G,X)$ sends f to the function

$$G^2 \to X, \quad (g_1, g_2) \mapsto g_1 \cdot f(g_2) - f(g_1 g_2) + f(g_1).$$

Its kernel $Z^1(G,X)$ consists of functions $f : G \to X$ satisfying

$$f(g_1 g_2) = f(g_1) + g_1 \cdot f(g_2),$$

called *crossed homomorphisms*. Thus $\mathbf{H}^1(G,X)$ is the quotient of the group of crossed homomorphisms by the group of functions of the form $g \mapsto gx - x$ for some $x \in X$ (which are called *principal crossed homomorphisms*). Note that if G acts trivially on X, then $\mathbf{H}^1(G,X) = \mathrm{Hom}(G,X)$.

Example 1.9.3. Let G be a group and X be an abelian group. By an *extension of G by X*, we mean a triple (E,i,p), where E is a group, $i : X \to E$ is an injective group homomorphism, $p : E \to G$ is a surjective homomorphism, such that $\ker p = \mathrm{im}\, i$. Given such an extension, we choose a set-theoretic section $s : G \to E$ of the map $p : E \to G$. For each $g \in G$, let g act on X by $x \mapsto s(g)xs(g)^{-1}$. This defines a G-module structure on X, which is independent of the choice of s. Consider the function $f : G^2 \to E, (g,h) \mapsto s(g)s(h)s(gh)^{-1}$. Since $p(f(g,h)) = gh(gh)^{-1} = 1$, we know that f is a function $G^2 \to X$. Moreover, one directly checks that $f \in Z^2(G,X)$, and its image in $\mathbf{H}^2(G,X)$ is independent of the choice of s. Note that the group structure on E is uniquely determined by the G-module X and f. Indeed, every element of E can be written as $xs(g)$ for unique $x \in X$ and $g \in G$. The multiplication is expressed as

$$x_1 s(g_1) x_2 s(g_2) = x_1 s(g_1) x_2 s(g_1)^{-1} s(g_1) s(g_2) = \big(x_1 (g_1 \cdot x_2) f(g_1, g_2)\big) s(g_1 g_2).$$

The expression on the right is again of the form $xs(g)$.

We define an isomorphism between two extensions (E,i,p) and (E',i',p') to be a group isomorphism $\phi : E \xrightarrow{\sim} E'$ such that $\phi \circ i = i'$ and $p' \circ \phi = p$. Then for any given G-module structure on X, the set $\mathbf{H}^2(G,X)$ classifies the isomorphism classes of extensions of G by X such that the induced G-module structure on X is the given one.

Suppose that $X \to Y$ is a map of G-modules. Then since $\mathbf{H}^i(G,\cdot)$ is a functor we have a homomorphism $\mathbf{H}^i(G,X) \to \mathbf{H}^i(G,Y)$. This can be described in terms of cochains as follows. We have an obvious map $C^i(G,X) \to C^i(G,Y)$ for each i, induced by the map $X \to Y$. These maps commute with the differentials, and hence induce maps $\mathbf{H}^i(G,X) \to \mathbf{H}^i(G,Y)$. These agree with the functorial maps.

Given a short exact sequence $0 \to X \to Y \to Z \to 0$ of G-modules, the connecting map $\delta : \mathbf{H}^i(G,Z) \to \mathbf{H}^{i+1}(G,X)$ can be described in terms of cochains as follows. Given $\alpha \in \mathbf{H}^i(G,Z)$, first find an i-cocycle $f : G^i \to Z$ representing α. Since $Y \to Z$ is surjective, we can lift f to an i-cochain $\tilde{f} : G^i \to Y$. Now $d\tilde{f}$ may no longer be 0, but we at least have $d\tilde{f} \in C^i(G,X)$ since for any $\underline{g} \in G^i$ the image of $(d\tilde{f})(\underline{g}) \in Y$ in Z is $(df)(\underline{g}) = 0$. Since $d(d\tilde{f}) = 0$, we have $d\tilde{f} \in Z^i(G,X)$. The class in $\mathbf{H}^i(G,X)$ represented by $d\tilde{f}$ is $\delta(\alpha)$.

Similarly, we can use the free resolution $P_\bullet \to \mathbb{Z} \to 0$ to compute $\mathbf{H}_i(G,X)$ and obtain the following explicit description. For $i \geq 0$ let $C_i(G,X)$ be the group of finitely supported functions $G^i \to X$. For $i \geq 1$ define the differential $d : C_i(G,X) \to C_{i-1}(G,X)$ by

$$\begin{aligned}(df)(g_1, \dots, g_{i-1}) &= \sum_{g \in G} g^{-1} f(g, g_1, \dots, g_{i-1}) + \\ &+ \sum_{j=1}^{i-1} (-1)^j \sum_{g \in G} f(g_1, \dots, g_{j-1}, g_j g, g^{-1}, g_{j+1}, \dots, g_{i-1}) + (-1)^i \sum_g f(g_1, \dots, g_{i-1}, g).\end{aligned}$$

Then $\mathbf{H}_i(G, X)$ is the i-th homology of the complex $C_\bullet(G, X)$.

1.10. **Computing $\mathbf{H}_1(G, \mathbb{Z})$.** Let $\mathbb{Z}$ be the $\mathbb{Z}[G]$-module with trivial G-action. We compute $\mathbf{H}_1(G, \mathbb{Z})$. Consider the *augmentation map*

$$\pi : \mathbb{Z}[G] \longrightarrow \mathbb{Z}, \quad \sum_g a_g[g] \longmapsto \sum_g a_g.$$

(This is the same as the map $\epsilon : P_0 \to \mathbb{Z}$ before.) Let I_G be the kernel of π. Note that I_G is a free $\mathbb{Z}$-module with basis $\{[1] - [g] \mid g \in G - \{1\}\}$. For any G-module X, we have

$$X_G \cong X/I_G X.$$

From the short exact sequence $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$, we obtain the long exact sequence

$$\mathbf{H}_1(G, \mathbb{Z}[G]) \to \mathbf{H}_1(G, \mathbb{Z}) \to \mathbf{H}_0(G, I_G) \to \mathbf{H}_0(G, \mathbb{Z}[G]).$$

The first term is zero since $\mathbb{Z}[G]$ is induced (Corollary 1.6.6), and the last map is zero since it is the map $I_G/I_G^2 \to \mathbb{Z}[G]/I_G$ induced by the inclusion $I_G \to \mathbb{Z}[G]$. Thus we have a canonical isomorphism

$$\mathbf{H}_1(G, \mathbb{Z}) \cong I_G/I_G^2.$$

Now it is elementary to check that

$$G \longrightarrow I_G/I_G^2, \quad g \mapsto 1 - [g]$$

induces an isomorphism $G^{\mathrm{ab}} \xrightarrow{\sim} I_G/I_G^2$. (Here G^{ab} is the abelianization of G as an abstract group.) Thus we have a canonical isomorphsm between $\mathbf{H}_1(G, \mathbb{Z})$ and G^{ab}.

1.11. **Change of group.** Suppose we have homomorphism of groups $\alpha : G' \to G$. For any G-module X, we obtain a G'-module $\alpha^* X$ whose underlying abelian group is X and the G'-action is given by $g'x := \alpha(g')x$. Clearly $X \mapsto \alpha^* X$ defines an exact functor from the category of G-modules to the category of G'-modules. Thus the family $(\mathbf{H}^i(G', \alpha^*(\cdot)))_{i \geq 0}$ is a (cohomological) δ-functor from G-modules to abelian groups. For $i = 0$, we have a natural transformation

$$\mathbf{H}^0(G, \cdot) \longrightarrow \mathbf{H}^0(G', \alpha^*(\cdot))$$

since for any G-module X, X^G is just a subgroup of $(\alpha^*(X))^{G'} = X^{\alpha(G')}$ and we have the inclusion map $X^G \hookrightarrow (\alpha^* X)^{G'}$. Thus by the universal property of derived functors this natural transformation extends uniquely to a morphism of δ-functors

$$\mathrm{Res}_\alpha : \big(\mathbf{H}^i(G, \cdot)\big)_i \longrightarrow \big(\mathbf{H}^i(G', \alpha^*(\cdot))\big)_i.$$

We call it *restriction along* α.

This construction can also be explicitly described as follows. For each i and each G-module X, pull-back via α defines a homomorphism

$$C^i(G, X) \longrightarrow C^i(G', \alpha^* X), \quad f \longmapsto \big((g'_1, \ldots, g'_i) \mapsto f(\alpha(g'_1), \ldots, \alpha(g'_i))\big).$$

These homomorphisms commute with the differentials $C^i(G, X) \to C^{i+1}(G, X)$ and $C^i(G', \alpha^* X) \to C^{i+1}(G', \alpha^* X)$, i.e., we have a morphism of complexes $C^\bullet(G, X) \to C^\bullet(G', \alpha^* X)$. So we get induced homomorphisms

$$\mathbf{H}^i(G, X) \longrightarrow \mathbf{H}^i(G', \alpha^* X).$$

These homomorphisms agree Res_α defined above.

The following two special cases are particularly important.

(1) Subgroup. Let $\alpha : H \hookrightarrow G$ be the inclusion of a subgroup. In this case the homomorphism $\mathbf{H}^i(G, X) \to \mathbf{H}^i(H, X)$ is called *restriction*, denoted by Res. At the cochain level, the map $C^i(G, X) \to C^i(H, X)$ is just restriction of a function $f : G^i \to X$ to H^i.

(2) Quotient group. Let N be a normal subgroup of G, and let $\alpha : G \to G/N$ be the quotient map. Then for every G/N-module X we have $\mathbf{H}^i(G/N, X) \to \mathbf{H}^i(G, X)$. Now for every G-module Y, note that Y^N is stable under the G-action since N is normal, and moreover the G-action factors through G/N. Thus Y^N is naturally a G/N-module. Consider the composite map

$$\mathbf{H}^i(G/N, Y^N) \to \mathbf{H}^i(G, Y^N) \to \mathbf{H}^i(G, Y),$$

where the second map is induced by the G-module map $Y^N \hookrightarrow Y$. This composite map is called *inflation*, denoted by Inf. At the cochain level, inflation sends $f : (G/N)^i \to Y^N$ to the composite map $G^i \to (G/N)^i \to Y^N \to Y$.

For homology, there is a similar construction. Again let $\alpha : G' \to G$ be a homomorphism. Then we have a natural transformation

$$\mathbf{H}_0(G', \alpha^*(\cdot)) \longrightarrow \mathbf{H}_0(G, \cdot)$$

(between functors from G-modules to abelian groups) since for every G-module X, X_G is a quotient group of $(\alpha^* X)_{G'} = X_{\alpha(G')}$. Again by the universal property of derived functors we obtain a unique extension to a morphism of δ-functors

$$\mathrm{Cor}_\alpha : \big(\mathbf{H}_i(G', \alpha^*(\cdot))\big)_i \longrightarrow \big(\mathbf{H}_i(G, \cdot)\big)_i.$$

We call it *corestriction along* α.

1.12. **The inflation-restriction sequence.** Let X be a G-module, and let N be a normal subgroup of G.

Proposition 1.12.1. *The sequence*

$$0 \to \mathbf{H}^1(G/N, X^N) \xrightarrow{\mathrm{Inf}} \mathbf{H}^1(G, X) \xrightarrow{\mathrm{Res}} \mathbf{H}^1(N, X)$$

is exact.

Proof. We first show the injectivity of Inf. Let $f \in Z^1(G/N, X^N)$. If $\mathrm{Inf}([f]) = 0$, then there exists $x \in X$ such that $f(\bar{g}) = x - gx$ for all $g \in G$. (Here $\bar{g}$ denotes the image of g in G/N.) But this equation already implies that $x \in X^N$ since the left hand side depends only on $\bar{g}$. Thus f is a coboundary in $Z^1(G/N, X^N)$.

We now show $\mathrm{Res} \circ \mathrm{Inf} = 0$. Let $f \in Z^1(G/N, X^N)$. Then $\mathrm{Res} \circ \mathrm{Inf}([f])$ is represented by the cocycle $f' : N \to X, n \mapsto f(\bar{n})$. But $f(\bar{n}) = f(1) = 0$ since $f(1 \cdot 1) = f(1) + 1 \cdot f(1)$. Hence $\mathrm{Res} \circ \mathrm{Inf}([f]) = 0$.

Finally, we show that $\ker(\mathrm{Res}) \subset \mathrm{im}(\mathrm{Inf})$. Let $f \in Z^1(G, X)$ represent a class in $\ker(\mathrm{Res})$. Then there exists $x \in X$ such that $f(n) = nx - x$ for all $n \in N$. Let $f' : G \to X, g \mapsto f(g) - gx + x$. Then $f' \in Z^1(G, X)$ and its class in $\mathbf{H}^1(G, X)$ is the same as that of f. It suffices to show that f' factors through G/N and lands in X^N, as then f' can be viewed as a cocycle in $Z^1(G/N, X^N)$ and its image under Inf is the original $[f]$. For this, note that $f'(n) = 0$ for all $n \in N$. Hence $f'(gn) = f'(g) + gf'(n) = f'(g)$ for all $g \in G, n \in N$. This shows that f' factors through G/N. For all $n \in N$ and $g \in G$, we have $f'(ng) = f'(n) + nf'(g) = nf'(g)$, and also $f'(ng) = f'(g)$ as we have already shown. This shows that $f'(g)$ is fixed by N, i.e., f' lands in X^N. □

We have the following generalization.

Proposition 1.12.2. *Let q be a positive integer. Suppose that $\mathbf{H}^i(N,X)=0$ for $1\le i\le q-1$. (If $q=1$, there is no hypothesis.) Then the sequence*

$$0\to \mathbf{H}^q(G/N,X^N)\xrightarrow{\text{Inf}}\mathbf{H}^q(G,X)\xrightarrow{\text{Res}}\mathbf{H}^q(N,X)$$

is exact.

For the proof we need the following two lemmas.

Lemma 1.12.3. *Let Y be a G-module, and let H be a subgroup of G. If Y is coinduced, then it is also coinduced when viewed as an H-module. Similarly for induced.*

Proof. Since $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module, we have an H-isomorphism $\mathbb{Z}[G]\cong\bigoplus_{i\in I}\mathbb{Z}[H]$ for some index set I, where H acts on the two sides via right multiplication. (Take I to be a set of representatives of G/H.) If $Y=\text{coInd}_1^G A$ for some abelian group A, then

$$Y=\text{Hom}_{\mathbb{Z}}(\mathbb{Z}[G],A)\cong\prod_{i\in I}\text{Hom}_{\mathbb{Z}}(\mathbb{Z}[H],A)\cong\text{Hom}_{\mathbb{Z}}(\mathbb{Z}[H],\prod_{i\in I}A)=\text{coInd}_1^H(\prod_{i\in I}A),$$

where the isomorphisms are H-equivariant. Thus Y is coinduced as an H-module.

To prove the statement about induced, we have an H-isomorphism $\mathbb{Z}[G]\cong\bigoplus_{j\in J}\mathbb{Z}[H]$ for some index set J, where H acts on the two sides via left multiplication. (Take J to be a set of representatives of $H\backslash G$.) If $Y=\text{Ind}_1^G A$, then

$$Y=\mathbb{Z}[G]\otimes_{\mathbb{Z}}A\cong\bigoplus_{i\in I}\left(\mathbb{Z}[H]\otimes_{\mathbb{Z}}A\right)\cong\mathbb{Z}[H]\otimes_{\mathbb{Z}}(\bigoplus_{i\in I}A)=\text{Ind}_1^H(\bigoplus_{i\in I}A),$$

where the isomorphisms are H-equivariant. Thus Y is induced as an H-module. □

Lemma 1.12.4. *Let Y be a coinduced G-module. Let N be a normal subgroup of G. Then Y^N is a coinduced G/N-module.*

Proof. Suppose $Y=\text{coInd}_1^G A=\text{Hom}_{\mathbb{Z}}(\mathbb{Z}[G],A)$. Thus Y is identified with the group of all set theoretic maps $G\to A$, and the G-action is given by right multiplication on G. Then Y^N consists of right N-invariant set theoretic maps $G\to A$, which are the same as maps $G/N\to A$. Hence Y^N is isomorphic to $\text{coInd}_1^{G/N}A$ as a G/N-module. □

Proof of Proposition 1.12.2. We induct on q. For $q=1$ this is Proposition 1.12.1. Assume $q\ge 2$. Recall that we have an injective G-homommorphism $X\hookrightarrow Y:=\text{coInd}_1^G X_0$, where X_0 is the underlying abelian group of X. Let $Z=\text{Cok}(X\to Y)$. Since Y is coinduced, we have $\mathbf{H}^i(G,Y)=0$ for all $i\ge 1$ (see Corollary 1.6.6). Thus by the long exact sequence associated with $0\to X\to Y\to Z\to 0$ we know that the connecting morphism induces an isomorphism

$$\delta:\mathbf{H}^i(G,Z)\xrightarrow{\sim}\mathbf{H}^{i+1}(G,X)$$

for $i\ge 1$.

Now since $\mathbf{H}^1(N,X)=0$ by hypothesis (as $q\ge 2$), the sequence

$$0\to X^N\to Y^N\to Z^N\to 0$$

is exact. By Lemma 1.12.4, Y^N is a coinduced G/N-module. Thus again we have

$$\delta:\mathbf{H}^i(G/N,Z^N)\xrightarrow{\sim}\mathbf{H}^{i+1}(G/N,X^N)$$

for $i\ge 1$.

Now if we view the G-module Y as an N-module, then it is also coinduced by Lemma 1.12.3. Then from the short exact sequence $0\to X\to Y\to Z\to 0$ of N-modules we obtain

$$\delta:\mathbf{H}^i(N,Z)\xrightarrow{\sim}\mathbf{H}^{i+1}(N,X)$$

for $i \geq 1$.

We have a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbf{H}^{q-1}(G/N, Z^N) & \xrightarrow{\text{Inf}} & \mathbf{H}^{q-1}(G, Z) & \xrightarrow{\text{Res}} & \mathbf{H}^{q-1}(N, Z) \\ & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} \\ 0 & \longrightarrow & \mathbf{H}^{q}(G/N, X^N) & \xrightarrow{\text{Inf}} & \mathbf{H}^{q}(G, X) & \xrightarrow{\text{Res}} & \mathbf{H}^{q}(N, X). \end{array}$$

We have already seen that the vertical maps are isomorphisms. To finish the proof, it suffices to check that the first row is exact. Note that Z satisfies the condition that $\mathbf{H}^i(N, Z) = 0$ for $1 \leq i \leq q-2$, since $\mathbf{H}^i(N, Z) \cong \mathbf{H}^{i+1}(N, X)$. Thus the first row of the above diagram is exact by the induction hypothesis. □

1.13. **Finite index subgroups.** Let $H \leq G$ be a finite index subgroup. In the following we define corestriction $\mathbf{H}^i(H, X) \to \mathbf{H}^i(G, X)$ and restriction $\mathbf{H}_i(G, X) \to \mathbf{H}_i(H, X)$ for any G-module X.

For $i = 0$, we define corestriction $\text{Cor} : \mathbf{H}^0(H, X) = X^H \to \mathbf{H}^0(G, X) = X^G$ as $x \mapsto \sum_{g \in G/H} gx$. The sum is finite and gx is well defined for $g \in G/H$ since x is fixed by H.

Now note that $(\mathbf{H}^i(H, \cdot))_i$ is a cohomological δ-functor from G-modules to abelian groups. We claim that these are actually the right derived functors of $\mathbf{H}^0(H, \cdot)$. (This does not directly follow from the definition since we are considering functors from G-modules, not H-modules, to abelian groups.) By Fact 1.4.5, it suffices to check that for any G-module X, there is a monomorphism $X \to I$ such that $\mathbf{H}^i(H, I) = 0$ for all $i \geq 1$. We have a monomorphism $X \to I = \text{coInd}_1^G X$. By Lemma 1.12.3, I is still coinduced as an H-module. Therefore $\mathbf{H}^i(H, I) = 0$ for all $i \geq 1$ as desired.

By the claim and the universal property for derived functors, $\text{Cor} : \mathbf{H}^0(H, \cdot) \to \mathbf{H}^0(G, \cdot)$ extends uniquely to a morphism between δ-functors (from G-modules to abelian groups)

$$\text{Cor} : \left(\mathbf{H}^i(H, \cdot)\right)_i \longrightarrow \left(\mathbf{H}^i(G, \cdot)\right)_i.$$

We follow a similar procedure to define restriction for homology. Let $\{g_i\}$ be a set of representatives for $H\backslash G$. Define $\text{Res} : \mathbf{H}_0(G, X) \to \mathbf{H}_0(H, X)$ as follows. Define $f : X \to X_H, x \mapsto \sum_i g_i x$. Clearly f is independent of the choice of $\{g_i\}$ since $hg_ix = hg_ix - g_ix + g_ix = g_ix$ in X_H, for any $h \in H$. Moreover, for any $g \in G$ and $x \in X$ we have $f(gx) = \sum_i g_i gx$, and by we have already seen this is equal to $f(x)$ since $\{g_i g\}_i$ is another set of representatives of $H\backslash G$. Thus f factors through X_G. We define Res to the map induced by f.

We now claim that the homological δ-functor $(\mathbf{H}_i(H, \cdot))_i$ from G-modules to abelian groups are actually the left derived functors of $\mathbf{H}_0(H, \cdot)$. By Fact 1.4.9, it suffices to check that for any G-module X, there is an epimorphism $P \to X$ such that $\mathbf{H}_i(H, P) = 0$ for all $i \geq 1$. We have an epimorphism $P = \text{Ind}_1^G X \to X$. By Lemma 1.12.3, P is still induced as an H-module. Therefore $\mathbf{H}_i(H, I) = 0$ for all $i \geq 1$ as desired.

By the claim and the universal property for left derived functors, $\text{Res} : \mathbf{H}_0(G, \cdot) \to \mathbf{H}_0(H, \cdot)$ extends uniquely to a morphism between δ-functors (from G-modules to abelian groups)

$$\text{Res} : \left(\mathbf{H}_i(G, \cdot)\right)_i \longrightarrow \left(\mathbf{H}_i(H, \cdot)\right)_i.$$

Let G be a group, and let H be a finite index subgroup of G.

Proposition 1.13.1. *Let X be a G-module. Then the compositions*

$$\mathbf{H}^i(G, X) \xrightarrow{\text{Res}} \mathbf{H}^i(H, X) \xrightarrow{\text{Cor}} \mathbf{H}^i(G, X)$$

and

$$\mathbf{H}_i(G,X) \xrightarrow{\text{Res}} \mathbf{H}_i(H,X) \xrightarrow{\text{Cor}} \mathbf{H}_i(G,X)$$

are both equal to multiplication by $[G:H]$.

Proof. We only prove the statement about cohomology, as the other one is proved similarly. When $i=0$ this follows immediately from the definition of Res and Cor. For general i, we prove the statement in two ways.

The first way uses dimension shifting as in the proof of Proposition 1.12.2. Thus we take a short exact sequence $0 \to X \to Y \to Z$ with Y coinduced (e.g. $Y = \text{coInd}_1^G X$). Then we have $\delta : \mathbf{H}^i(G,Z) \xrightarrow{\sim} \mathbf{H}^{i+1}(G,X)$ and $\delta : \mathbf{H}^i(H,Z) \xrightarrow{\sim} \mathbf{H}^{i+1}(G,X)$ as in that proof. These isomorphisms commute with Res and Cor. Thus the statement for (X,i) follows from the induction hypothesis for $(Z,i-1)$.

Alternatively, we observe that $\text{Cor} \circ \text{Res}$ and multiplication by $[G:H]$ are two morphisms from the δ-functor $(\mathbf{H}^i(G,\cdot))$ to itself. They agree on $\mathbf{H}^0$, so they must agree for all i by the universal property (the uniqueness of extending a natural transformation defined on $\mathbf{H}^0$). □

Corollary 1.13.2. *If G is finite, then $\mathbf{H}^i(G,X)$ and $\mathbf{H}_i(G,X)$ are killed by $|G|$ for $i \geq 1$.*

Proof. The composition $\mathbf{H}^i(G,X) \xrightarrow{\text{Res}} \mathbf{H}^i(\{1\},X) \xrightarrow{\text{Cor}} \mathbf{H}^i(G,X)$ is equal to $|G|$, and it is zero since the middle group is zero. Similarly for homology. □

Corollary 1.13.3. *If G is finite and X is a G-module which is finitely generated as an abelian group, then $\mathbf{H}^i(G,X)$ and $\mathbf{H}_i(G,X)$ are finite abelian groups killed by $|G|$ for $i \geq 1$.*

Proof. For all i, $C^i(G,X)$ and $C_i(G,X)$ are isomorphic to the direct sum of $|G|^i$ copies of X as an abelian group, and in particular finitely generated. Therefore $\mathbf{H}^i(G,X)$ and $\mathbf{H}_i(G,X)$ are finitely generated abelian groups. For $i \geq 1$, they are killed by $|G|$, so they must be finite. □

An important special case of restriction for homology is the homomorphism

$$\text{Res} : \mathbf{H}_1(G,\mathbb{Z}) \longrightarrow \mathbf{H}_1(H,\mathbb{Z})$$

when $H \leq G$ is of finite index. Recall that the two sides are canonically identified with G^{ab} and H^{ab}. The resulting homomorphism $G^{\text{ab}} \to H^{\text{ab}}$ is called *transfer*, and it can be described by an explicit formula as follows.

Proposition 1.13.4. *Fix a section $\theta : H\backslash G \to G$ of the projection $G \to H\backslash G$. For each $s \in G$ and $t \in H\backslash G$, define $x_{t,s} \in H$ by*

$$\theta(t)s = x_{t,s}\theta(ts).$$

Then the transfer map $G^{\text{ab}} \to H^{\text{ab}}$ is induced by

$$G \longrightarrow H, \quad s \longmapsto \prod_{t \in H\backslash G} x_{t,s}.$$

Exercise 1.13.5. Prove Proposition 1.13.4.

1.14. **Tate cohomology.** From now on, let G be a fintie group. For any G-module X, we have the *norm map*

$$\mathrm{N}_G : X \longrightarrow X, \quad x \longmapsto \sum_{g\in G} g\cdot x.$$

We write $X[\mathrm{N}_G]$ for $\ker(\mathrm{N}_G : X \to X)$. Recall that $\mathbf{H}^0(G,X) = X^G$ and $\mathbf{H}_0(G,X) = X_G = X/I_GX$. It is easy to see that

$$\mathrm{N}_G(X) \subset X^G, \quad I_GX \subset X[\mathrm{N}_G].$$

Define

$$\widehat{\mathbf{H}}^0(G,X) := X^G/\mathrm{N}_G(X)$$

and

$$\widehat{\mathbf{H}}^{-1}(G,X) := X[\mathrm{N}_G]/I_GX.$$

Thus $\widehat{\mathbf{H}}^0(G,X)$ is a quotient group of $\mathbf{H}^0(G,X)$, and $\widehat{\mathbf{H}}^{-1}(G,X)$ is a subgroup of $\mathbf{H}_0(G,X)$.

Also define

$$\widehat{\mathbf{H}}^i(G,X) := \begin{cases} \mathbf{H}^i(G,X), & i \geq 1, \\ \mathbf{H}_{-i-1}(G,X), & i \leq -2. \end{cases}$$

The family $\widehat{\mathbf{H}}^i(G,X)$ for $i \in \mathbb{Z}$ are called the *Tate cohomology groups*.

Let $0 \to X \to Y \to Z \to 0$ be a short exact sequence of G-modules. We shall construct a long exact sequence

$$\cdots \to \widehat{\mathbf{H}}^i(G,X) \to \widehat{\mathbf{H}}^i(G,Y) \to \widehat{\mathbf{H}}^i(G,Z) \xrightarrow{\delta^i} \widehat{\mathbf{H}}^{i+1}(G,X) \to \cdots \tag{1.2}$$

where i runs over all integers. For $i \geq 1$, define δ^i to be the usual connecting homomorphism for cohomology $\mathbf{H}^i(G,Z) \to \mathbf{H}^{i+1}(G,X)$. For $i \leq -3$, define δ^i to be the usual connecting homomorphism for homology $\mathbf{H}_{-i-1}(G,Z) \to \mathbf{H}_{-i-2}(G,X)$.

For $i = 0$, we check that the usual connecting homomorphism $\delta : \mathbf{H}^0(G,Z) \to \mathbf{H}^1(G,X)$ factors through the quotient $\mathbf{H}^0(G,Z) \to \widehat{\mathbf{H}}^0(G,Z)$, and then define δ^0 to be the induced map $\widehat{\mathbf{H}}^0(G,Z) \to \mathbf{H}^1(G,X) = \widehat{\mathbf{H}}^1(G,X)$. Indeed, the image of $\mathrm{N}_G : Z \to Z^G$ lies in the image of $Y^G \to Z^G$ since for any $z \in Z$, we can find a preimage $y \in Y$ and then we have $\mathrm{N}_G(z) \in Z^G$ is the image of $\mathrm{N}_G(y) \in Y^G$. Thus the desired factoring of $\delta : \mathbf{H}^0(G,Z) \to \mathbf{H}^1(G,X)$ follows from the fact that the composition $\mathbf{H}^0(G,Y) \to \mathbf{H}^0(G,Z) \to \mathbf{H}^1(G,X)$ is zero.

Similarly, for $i = -2$ one checks that the usual connecting homomorphism $\mathbf{H}_1(G,Z) \to \mathbf{H}_0(G,X)$ has image in the subgroup $\widehat{\mathbf{H}}^{-1}(G,X) \subset \mathbf{H}_0(G,X)$ (which we omit). We then define δ^{-2} to be the induced map $\widehat{\mathbf{H}}^{-2}(G,Z) = \mathbf{H}_1(G,Z) \to \widehat{\mathbf{H}}^{-1}(G,X)$.

To define $\delta^{-1} : \widehat{\mathbf{H}}^{-1}(G,Z) \to \widehat{\mathbf{H}}^0(G,X)$, we apply snake lemma to the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} & & X_G & \longrightarrow & Y_G & \longrightarrow & Z_G \longrightarrow 0 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} \\ 0 & \longrightarrow & X^G & \longrightarrow & Y^G & \longrightarrow & Z^G \end{array}$$

where the vertical maps f_i are induced by the norm maps $\mathrm{N}_G : X \to X^G$ (which factors through the quotient $X \to X_G$), $\mathrm{N}_G : Y \to Y^G$, and $\mathrm{N}_G : Z \to Z^G$. Then we obtain an exact sequence

$$\ker f_1 \to \ker f_2 \to \ker f_3 \xrightarrow{\delta} \mathrm{Cok} f_1 \to \mathrm{Cok} f_2 \to \mathrm{Cok} f_3.$$

(Recall that δ is defined as follows: For any $z \in \ker f_3$, find a lift $y \in Y_G$. Then $f_2(y)$ comes from a unique element $x \in X^G$. Define $\delta(z)$ to be the image of x.) Note that $\ker f_1 = \widehat{\mathbf{H}}^{-1}(G, X), \mathrm{Cok} f_1 = \widehat{\mathbf{H}}^0(G, X)$, and similarly for X replaced by Y and Z. Thus we obtain an exact sequence

$$\widehat{\mathbf{H}}^{-1}(G, X) \to \widehat{\mathbf{H}}^{-1}(G, Y) \to \widehat{\mathbf{H}}^{-1}(G, Z) \xrightarrow{\delta} \widehat{\mathbf{H}}^0(G, X) \to \widehat{\mathbf{H}}^0(G, Y) \to \widehat{\mathbf{H}}^0(G, Z).$$

We define δ^{-1} to be δ in the above.

It is clear from the definition that (1.2) is a long exact sequence. Moreover, this long exact sequence depends functorially on the short exact sequence $0 \to X \to Y \to Z \to 0$.

Recall that since G is finite, coinduced G-modules are the same as induced G-modules. Thus relatively injective G-modules are the same as relatively projective G-modules, i.e., they are direct summands of (co)induced G-modules.

Lemma 1.14.1. *Let X be a relatively injective G-module. Then $\widehat{\mathbf{H}}^i(G, X) = 0$ for all $i \in \mathbb{Z}$.*

Proof. If $i \neq 0, -1$, then this is just Corollary 1.6.6. For $i = 0$ or -1, we may assume that $X = \mathrm{Ind}_1^G A$. Then $X \cong \bigoplus_{g \in G} A$, and G acts on X by permuting the coordinates. We have

$$X^G = \{(a_g)_{g \in G} \mid a_g = a_h, \forall g, h \in G\}.$$

Any element $(a_g)_{g \in G}$ of it can be written as $\mathrm{N}_G((a_1, 0, \cdots, 0))$. Hence $X^G = \mathrm{N}_G(X)$. Also

$$X[\mathrm{N}_G] = \{(a_g)_{g \in G} \mid \sum a_g = 0\}.$$

Any element $(a_g)_{g \in G}$ of it is equal to

$$\sum_{g \in G - \{1\}} (-a_g, 0, \cdots, 0, a_g, 0, \cdots, 0),$$

where $-a_g$ appears at the coordinate corresponding to $1 \in G$, and a_g appears at the coordinate corresponding to $g \in G$. Now each summand clearly lies in $I_G X$, so $X[\mathrm{N}_G] = I_G X$. □

Given any G-module X, we know that there is monomorphism of G-modules $X \to I$ and an epimorphism of G-modules $P \to X$, where I and P are induced G-modules. In view of Lemma 1.14.1, the connecting homomorphisms are isomorphisms $\widehat{\mathbf{H}}^{i-1}(G, I/X) \xrightarrow{\sim} \widehat{\mathbf{H}}^i(G, X)$ and $\widehat{\mathbf{H}}^i(G, X) \xrightarrow{\sim} \widehat{\mathbf{H}}^{i+1}(G, \ker(P \to X))$. Using this one can often make a dimension shifting argument, reducing the study of $\widehat{\mathbf{H}}^i(G, X)$ to that of $\widehat{\mathbf{H}}^{i-1}(G, I/X)$ or $\widehat{\mathbf{H}}^{i+1}(G, \ker(P \to X))$. For instance, a statement about arbitrary $i \in \mathbb{Z}$ may be reduced to the case $i = 0$.

We now discuss an alternative and equivalent way to define Tate cohomology. Since G is finite, there is a free resolution $P_\bullet \xrightarrow{\epsilon} \mathbb{Z} \to 0$ in the category of G-modules such that each P_i is a finite rank free abelian group. For instance, the standard free resolution in Proposition 1.7.1 satisfies this property. For any finite rank free abelian group P, we write $P^\vee$ for $\mathrm{Hom}_{\mathbb{Z}}(P, \mathbb{Z})$. Then $P^\vee$ is also finite rank free and we have $(P^\vee)^\vee = P$. If P is in addition a free $\mathbb{Z}[G]$-module, then $P^\vee$ is also a free $\mathbb{Z}[G]$-module.

Consider the sequence

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} \mathbb{Z} \cong \mathbb{Z}^\vee \xrightarrow{\epsilon^\vee} P_0^\vee \xrightarrow{d_1^\vee} P_1^\vee \xrightarrow{d_2^\vee} P_2^\vee \to \cdots$$

We set $P_{-1} := P_0^\vee, P_{-2} := P_1^\vee$, etc. Then we obtain a complex $(P_\bullet)_{\bullet \in \mathbb{Z}}$, where the differential $P_0 \to P_{-1}$ is the composition $\epsilon^\vee \circ \epsilon$. This is called a *complete resolution of* $\mathbb{Z}$. (More precisely, $(P_\bullet)_{\bullet \in \mathbb{Z}}$ together with the maps $\epsilon : P_0 \to \mathbb{Z}$ and $\epsilon^\vee : \mathbb{Z} \to P_{-1}$ is called a complete resolution of $\mathbb{Z}$.)

Fact 1.14.2. *For any G-module X, $\widehat{\mathbf{H}}^i(G,X)$ is the i-th cohomology of the complex*

$$\big(\mathrm{Hom}_{\mathbb{Z}[G]}(P_\bullet, X)\big)_{\bullet\in\mathbb{Z}}.$$

From this point of view it is easy to understand the long exact sequence attached to a short exact sequence. Namely, for each $i \in \mathbb{Z}$, the functor $\mathrm{Hom}_{\mathbb{Z}[G]}(P_i, \cdot)$ is exact. Hence if $0 \to X \to Y \to Z \to 0$ is a short exact sequence of G-modules, we obtain a short exact sequence of complexes

$$0 \to \big(\mathrm{Hom}_{\mathbb{Z}[G]}(P_\bullet, X)\big)_{\bullet\in\mathbb{Z}} \to \big(\mathrm{Hom}_{\mathbb{Z}[G]}(P_\bullet, Y)\big)_{\bullet\in\mathbb{Z}} \to \big(\mathrm{Hom}_{\mathbb{Z}[G]}(P_\bullet, Z)\big)_{\bullet\in\mathbb{Z}} \to 0$$

giving rise to a long exact sequence of the cohomology.

Proposition 1.14.3 (Shapiro's Lemma for Tate cohomology)**.** *Let H be a subgroup of G. For each H-module X, there are natural isomorphisms*

$$\widehat{\mathbf{H}}^i(G, \mathrm{Ind}_H^G X) \cong \widehat{\mathbf{H}}^i(H, X)$$

for all $i \in \mathbb{Z}$.

Proof. The proof is similar to the proof of Proposition 1.6.4, using complete resolution to compute Tate cohomology. □

1.15. **Restriction and corestriction for Tate cohomology.** Let G be a finite group, and $H \leq G$ a subgroup. We have defined $\mathrm{Res} : \mathbf{H}^i(G,\cdot) \to \mathbf{H}^i(H,\cdot)$ and $\mathrm{Res} : \mathbf{H}_i(G,\cdot) \to \mathbf{H}_i(H,\cdot)$ for all $i \geq 0$. One checks that the composite map $\mathbf{H}^0(G,\cdot) \xrightarrow{\mathrm{Res}} \mathbf{H}^0(H,\cdot) \to \widehat{\mathbf{H}}^0(H,\cdot)$ factors through a map $\mathrm{Res} : \widehat{\mathbf{H}}^0(G,\cdot) \to \widehat{\mathbf{H}}^0(H,\cdot)$, and that $\mathrm{Res} : \mathbf{H}_0(G,\cdot) \to \mathbf{H}_0(H,\cdot)$ restrict to a map $\mathrm{Res} : \widehat{\mathbf{H}}^{-1}(G,\cdot) \to \widehat{\mathbf{H}}^{-1}(H,\cdot)$. Thus we have

$$\mathrm{Res} : \widehat{\mathbf{H}}^i(G,\cdot) \longrightarrow \widehat{\mathbf{H}}^i(H,\cdot)$$

for all $i \in \mathbb{Z}$. Moreover, we have the following characterization.

Proposition 1.15.1. *We have a family of natural transformations $\mathrm{Res} : \widehat{\mathbf{H}}^i(G,\cdot) \to \widehat{\mathbf{H}}^i(H,\cdot)$, for all $i \in \mathbb{Z}$, and this family is uniquely characterized by the following properties:*

1. *For each G-module X, the map $\mathrm{Res} : \widehat{\mathbf{H}}^0(G,X) \to \widehat{\mathbf{H}}^0(H,X)$ is induced by the usual corestriction map $X^G \to X^H$.*
2. *These natural transformations are compatible with the connecting homomorphisms.*

Proof. The uniqueness follows from dimension shifting. To prove that Res indeed satisfies condition (ii), we need to check that for a short exact sequence $0 \to A \to B \to C \to 0$, we have a commutative diagram

$$\begin{array}{ccc} \widehat{\mathbf{H}}^i(G,C) & \xrightarrow{\delta} & \widehat{\mathbf{H}}^{i+1}(G,A) \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} \\ \widehat{\mathbf{H}}^i(H,C) & \xrightarrow{\delta} & \widehat{\mathbf{H}}^{i+1}(H,A) \end{array}$$

Only the case $i = -1$ is essentially new. But in this case the compatibility can be checked using the explicit description of δ. □

Similarly, we have corestriction

$$\mathrm{Cor} : \widehat{\mathbf{H}}^i(H,\cdot) \longrightarrow \widehat{\mathbf{H}}^i(G,\cdot)$$

for all $i \in \mathbb{Z}$. For $i \neq 0, -1$, this is the usual corestriction for cohomology or homology. For $i = -1$, one checks that $\mathrm{Cor} : \mathbf{H}_0(H,\cdot) \to \mathbf{H}_0(G,\cdot)$ restricts to a map $\mathrm{Cor} : \widehat{\mathbf{H}}^{-1}(H,\cdot) \to$

$\widehat{\mathbf{H}}^{-1}(G,\cdot)$. For $i=0$, one checks that the composite map $\mathbf{H}_0(H,\cdot)\xrightarrow{\mathrm{Cor}}\mathbf{H}^0(G,\cdot)\to\widehat{\mathbf{H}}^0(G,\cdot)$ factors through a map $\mathrm{Cor}:\widehat{\mathbf{H}}^0(H,\cdot)\to\widehat{\mathbf{H}}^0(G,\cdot)$. Similarly as before, corestriction is characterized as follows.

Proposition 1.15.2. *We have a family of natural transformations* $\mathrm{Cor}:\widehat{\mathbf{H}}^i(G,\cdot)\to\widehat{\mathbf{H}}^i(H,\cdot)$, *for all* $i\in\mathbb{Z}$, *and this family is uniquely characterized by the following properties:*

(1) *For each* G*-module* X, *the map* $\mathrm{Cor}:\widehat{\mathbf{H}}^0(H,X)\to\widehat{\mathbf{H}}^0(G,X)$ *is induced by the norm map* $\mathrm{N}_{G/H}:X^H\to X^G$.
(2) *These natural transformations are compatible with the connecting homomorphisms.*

Corollary 1.15.3. *For each* $i\in\mathbb{Z}$, *the composition*

$$\widehat{\mathbf{H}}^i(G,\cdot)\xrightarrow{\mathrm{Res}}\widehat{\mathbf{H}}^i(H,\cdot)\xrightarrow{\mathrm{Cor}}\widehat{\mathbf{H}}^i(G,\cdot)$$

is equal to multiplication by $[G:H]$.

Proof. Check this for $i=0$ explicitly, and prove the general case by dimension shifting. □

Exercise 1.15.4. For any abelian group A viewed as a G-module for the trivial group $G=\{1\}$, we have $\widehat{\mathbf{H}}^i(\{1\},A)=0$ for all $i\in\mathbb{Z}$.

Corollary 1.15.5. *For each* $i\in\mathbb{Z}$, *the abelian group* $\widehat{\mathbf{H}}^i(G,X)$ *is killed by* $|G|$. *It is finite if* X *is finitely generated as an abelian group.*

Proof. Take H to be trivial in Corollary 1.15.3, and use Exercise 1.15.4. □

1.16. **Cup product.** We continue letting G be a finite group. For G-modules A and B, we define a G-module structure on $A\otimes B=A\otimes_{\mathbb{Z}}B$ by $g\cdot(a\otimes b)=ga\otimes gb$.

Proposition 1.16.1. *There is a unique family of* $\mathbb{Z}$*-bilinear pairings:*

$$\cup:\widehat{\mathbf{H}}^p(G,A)\otimes\widehat{\mathbf{H}}^q(G,B)\longrightarrow\widehat{\mathbf{H}}^{p+q}(G,A\otimes B),\quad p,q\in\mathbb{Z}$$

satisfying the following conditions:

(1) *Functoriality in* A *and* B. *For instance, functoriality in* A *means the following: For any morphism* $f:A\to A'$ *of* G*-modules, we have a commutative diagram*

$$\begin{array}{ccc}\widehat{\mathbf{H}}^p(G,A)\otimes\widehat{\mathbf{H}}^q(G,B) & \xrightarrow{\cup} & \widehat{\mathbf{H}}^{p+q}(G,A\otimes B)\\ \downarrow{\scriptstyle\widehat{\mathbf{H}}^p(G,\cdot)(f)\otimes\mathrm{id}} & & \downarrow{\scriptstyle\widehat{\mathbf{H}}^{p+q}(G,\cdot)(f\otimes\mathrm{id})}\\ \widehat{\mathbf{H}}^p(G,A')\otimes\widehat{\mathbf{H}}^q(G,B) & \xrightarrow{\cup} & \widehat{\mathbf{H}}^{p+q}(G,A'\otimes B)\end{array}$$

(2) *For* $p=q=0$, *this is induced by the natural map* $A^G\otimes B^G\to(A\otimes B)^G$ *by passing to quotients.*
(3) *Suppose* $0\to A\to A'\to A''\to 0$ *is a short exact sequence of* G*-modules, and* B *is a* G*-module such that* $0\to A\otimes B\to A'\otimes B\to A''\otimes B\to 0$ *is still exact. Then for each* $\beta\in\widehat{\mathbf{H}}^q(G,B)$ *the following diagram commutes:*

$$\begin{array}{ccc}\widehat{\mathbf{H}}^p(G,A'') & \xrightarrow{\delta} & \widehat{\mathbf{H}}^{p+1}(G,A)\\ \downarrow{\scriptstyle\cdot\cup\beta} & & \downarrow{\scriptstyle\cdot\cup\beta}\\ \widehat{\mathbf{H}}^{p+q}(G,A''\otimes B) & \xrightarrow{\delta} & \widehat{\mathbf{H}}^{p+q+1}(G,A\otimes B)\end{array}$$

(4) *Suppose* $0 \to B \to B' \to B'' \to 0$ *and* $0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0$ *are exact. Then for each* $\alpha \in \widehat{\mathbf{H}}^p(G, A)$ *the following diagram commutes*

$$\begin{array}{ccc} \widehat{\mathbf{H}}^q(G, B'') & \xrightarrow{\delta} & \widehat{\mathbf{H}}^{q+1}(G, B) \\ \downarrow{\scriptstyle (-1)^p \alpha \cup \cdot} & & \downarrow{\scriptstyle \alpha \cup \cdot} \\ \widehat{\mathbf{H}}^{p+q}(G, A \otimes B'') & \xrightarrow{\delta} & \widehat{\mathbf{H}}^{p+q+1}(G, A \otimes B) \end{array}$$

Proof. The uniqueness follows from dimension shifting. See [CF+67, §IV.7] or [Bro94, §VI.5] for the proof of existence. □

Proposition 1.16.2. *The cup product satisfies the following properties. Let* A, B, C *be* G*-modules. Let* $a \in \widehat{\mathbf{H}}^p(G, A), b \in \widehat{\mathbf{H}}^q(G, B), c \in \widehat{\mathbf{H}}^r(G, C)$.

(1) *We have*
$$(a \cup b) \cup c = a \cup (b \cup c)$$
under the identification $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$.
(2) *We have* $a \cup b = (-1)^{pq} b \cup a$ *under the identification* $A \otimes B \cong B \otimes A$.
(3) *Let* $H \leq G$. *Then* $\mathrm{Res}(a \cup b) = \mathrm{Res}(a) \cup \mathrm{Res}(b)$, *and* $\mathrm{Cor}(a' \cup \mathrm{Res}(b)) = \mathrm{Cor}(a') \cup b$ *for all* $a' \in \widehat{\mathbf{H}}^p(H, A)$.

Proof. All the properties can be checked directly for the cup product between $\widehat{\mathbf{H}}^0$. The general case is then proved by dimension shifting. For instance, let us check $\mathrm{Cor}(a' \cup \mathrm{Res}(b)) = \mathrm{Cor}(a') \cup b$ for $a' \in \widehat{\mathbf{H}}^0(H, A)$ and $b \in \widehat{\mathbf{H}}^0(G, B)$. We lift a' to an element $a' \in A^H$, and lift b to an element $b \in B^G$. Then $\mathrm{Cor}(a' \cup \mathrm{Res}(b))$ is represented by

$$\sum_{g \in G/H} ga' \otimes gb = \sum_{g \in G/H} ga' \otimes b = \Big(\sum_{g \in G/H} ga'\Big) \otimes b.$$

But $\sum_{g/H} ga' \in A^G$ represents $\mathrm{Cor}(a')$. The desired identify follows. □

1.17. **Cohomology of a finite cyclic group.** Let G be a finite cyclic group of order n. The main result about cohomology of G is Theorem 1.17.2 below. Our approach follows [CF+67, §IV.8]. See [Ser79, §VIII.4] for a different point of view.

By definition, we have $\widehat{\mathbf{H}}^0(G, \mathbb{Z}) = \mathbb{Z}^G / \mathrm{N}_G(\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$.

Lemma 1.17.1. *Let* $x \in \widehat{\mathbf{H}}^0(G, \mathbb{Z}) = \mathbb{Z}/n$ *be a generator. Then* $x \cup \cdot$ *defines an automorphism of* $\widehat{\mathbf{H}}^i(G, A)$ *for each* $i \in \mathbb{Z}$ *and each* G*-module* A. *(Here we identify* $\mathbb{Z} \otimes A$ *with* A.*)*

Proof. By dimension shifting, we reduce to the case $i = 0$. (To give more details, suppose $i > 0$. Find a short exact sequence $0 \to A \to P \to A' \to 0$ with P induced. Then the connecting homomorphism $\widehat{\mathbf{H}}^{i-1}(G, A') \to \widehat{\mathbf{H}}^i(G, A)$ is an isomorphism. This isomorphism is compatible with the endomorphisms on the two groups provided by $x \cup \cdot$. Thus we can lower i and reduce to the case $i = 0$. If $i < 0$, we find a short exact sequence $0 \to A' \to P \to A \to 0$ with P induced and argue similarly.)

When $i = 0$, the map in question is scalar multiplication by $x \in \mathbb{Z}/n$ on the $\mathbb{Z}/n$-module $\widehat{\mathbf{H}}^0(G, A)$. Since $x \in (\mathbb{Z}/n)^\times$, this map is an automorphism. □

Theorem 1.17.2. *The group* $\widehat{\mathbf{H}}^2(G, \mathbb{Z})$ *is cyclic of order* n. *Let* $x \in \widehat{\mathbf{H}}^2(G, \mathbb{Z})$ *be a generator. Then* $x \cup \cdot$ *defines an isomorphism* $\widehat{\mathbf{H}}^i(G, A) \to \widehat{\mathbf{H}}^{i+2}(G, A)$ *for each* $i \in \mathbb{Z}$ *and each*

G-module A. In particular, the isomorphism class of $\widehat{\mathbf{H}}^i(G,A)$ is periodic in i with period 2.

Proof. We have a short exact sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0,$$

where the last map is the augmentation map $\sum_g a_g[g] \mapsto \sum_g a_g$. Let s be a generator of G. We then have a short exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Z}[G] \to I_G \to 0,$$

where the two maps are multiplication by $\sum_{g\in G}[g]$ and by $1-[s]$ respectively. (To see that the map $\mathbb{Z}[G] \to I_G$ is surjective, use that $1-[s^k] = (1-[s])(1+[s]+\cdots+[s^{k-1}])$.) From these two short exact sequences, we obtain connecting homomorphisms

$$\delta_1 : \widehat{\mathbf{H}}^0(G,\mathbb{Z}) \xrightarrow{\sim} \widehat{\mathbf{H}}^1(G,I_G)$$

and

$$\delta_2 : \widehat{\mathbf{H}}^1(G,I_G) \xrightarrow{\sim} \widehat{\mathbf{H}}^2(G,\mathbb{Z})$$

both of which are isomorphisms since $\mathbb{Z}[G]$ is induced. It follows that $\widehat{\mathbf{H}}^2(G,\mathbb{Z}) \cong \widehat{\mathbf{H}}^0(G,\mathbb{Z})$ is cyclic of order n.

Note that the two short exact sequences above remain exact after tensoring with A, since the abelian groups I_G and $\mathbb{Z}$ are free. Also, $\mathbb{Z}[G]\otimes A$ is an induced G-module. Indeed, we have an isomorphism of G-modules $\mathrm{Ind}_1^G A_0 = \mathbb{Z}[G]\otimes A_0 \xrightarrow{\sim} \mathbb{Z}[G]\otimes A, [g]\otimes a \mapsto [g]\otimes ga$, where A_0 is the underlying abelian group of A equipped with the trivial G-action. Hence we obtain connecting homomorphisms

$$\delta_{1,A} : \widehat{\mathbf{H}}^i(G,A) \xrightarrow{\sim} \widehat{\mathbf{H}}^{i+1}(G, I_G\otimes A)$$

and

$$\delta_{2,A} : \widehat{\mathbf{H}}^{i+1}(G,I_G) \xrightarrow{\sim} \widehat{\mathbf{H}}^{i+2}(G,A)$$

which are isomorphisms. For any $y \in \widehat{\mathbf{H}}^i(G,A)$, we have a commutative diagram

$$\begin{array}{ccccc}
\widehat{\mathbf{H}}^0(G,\mathbb{Z}) & \xrightarrow[\sim]{\delta_1} & \widehat{\mathbf{H}}^1(G,I_G) & \xrightarrow[\sim]{\delta_2} & \widehat{\mathbf{H}}^2(G,\mathbb{Z}) \\
\downarrow{\scriptstyle \cdot\cup y} & & \downarrow{\scriptstyle \cdot\cup y} & & \downarrow{\scriptstyle \cdot\cup y} \\
\widehat{\mathbf{H}}^i(G,A) & \xrightarrow[\sim]{\delta_{1,A}} & \widehat{\mathbf{H}}^{i+1}(G,I_G\otimes A) & \xrightarrow[\sim]{\delta_{2,A}} & \widehat{\mathbf{H}}^{i+2}(G,A)
\end{array}$$

Thus if x is a generator of $\widehat{\mathbf{H}}^2(G,\mathbb{Z})$ and we set $x_0 = \delta_1^{-1}(\delta_2^{-1}(x))$, then

$$x\cup y = \delta_{2,A}(\delta_{1,A}(x_0\cup y))$$

for all $y \in \widehat{\mathbf{H}}^i(G,A)$. Hence in order to show that $x\cup\cdot$ is an isomorphism $\widehat{\mathbf{H}}^i(G,A) \xrightarrow{\sim} \widehat{\mathbf{H}}^{i+2}(G,A)$ it suffices to show that $x_0\cup\cdot$ is an automorphism of $\widehat{\mathbf{H}}^i(G,A)$. Since x_0 is a generator of $\widehat{\mathbf{H}}^0(G,\mathbb{Z})$, this is Lemma 1.17.1. □

Remark 1.17.3. In the proof we have an isomorphism $\delta_{2,A}\circ\delta_{1,A} : \widehat{\mathbf{H}}^i(G,A) \xrightarrow{\sim} \widehat{\mathbf{H}}^{i+2}(G,A)$. Note that this is not canonical as $\delta_{2,A}$ depends on the choice of generator $s\in G$. Of course the choice of s gives rise to a choice of generator $x \in \widehat{\mathbf{H}}^2(G,\mathbb{Z})$, namely the image under $\delta_2\circ\delta_1$ of $\bar{1} \in \widehat{\mathbf{H}}^0(G,\mathbb{Z}) = \mathbb{Z}/n$, and the isomorphism $\delta_{2,A}\circ\delta_{1,A}$ is the same as $x\cup\cdot$ as the proof shows. Thus one can think that by either choosing a generator $s\in G$ or choosing a generator $x\in\widehat{\mathbf{H}}^2(G,\mathbb{Z})$ one obtains an isomorphism $\widehat{\mathbf{H}}^i(G,A) \xrightarrow{\sim} \widehat{\mathbf{H}}^{i+2}(G,A)$. The latter

point of view has the advantage that the isomorphism $x\cup\cdot$ is defined without using any extra knowledge about the group G, and hence can be analyzed more formally in applications.

Definition 1.17.4. For every G-module A, we write $h^q(A)$ for the cardinality of $\widehat{\mathbf{H}}^q(G,A)$ whenever it is finite. Define the *Herbrand quotient* to be $h(A)=h^0(A)/h^1(A)$ when $h^0(A)$ and $h^1(A)$ are both defined.

Example 1.17.5. We have $\widehat{\mathbf{H}}^0(G,\mathbb{Z})=\mathbb{Z}/|G|\mathbb{Z}$ and $\widehat{\mathbf{H}}^{-1}(G,\mathbb{Z})=0$. Hence $h(\mathbb{Z})=|G|$.

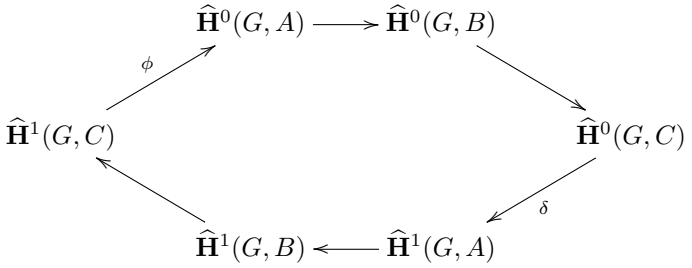
Proposition 1.17.6. *Let $0\to A\to B\to C\to 0$ be a short exact sequence of G-modules. If two of $h(A),h(B),h(C)$ are defined, then so is the third, and we have $h(B)=h(A)h(C)$.*

Proof. Fix a generator $x\in\widehat{\mathbf{H}}^2(G,\mathbb{Z})$. The following compositions are equal:

$$\widehat{\mathbf{H}}^1(G,C)\xrightarrow{(x\cup\cdot)^{-1}}\widehat{\mathbf{H}}^{-1}(G,C)\xrightarrow{\delta}\widehat{\mathbf{H}}^0(G,A),$$

$$\widehat{\mathbf{H}}^1(G,C)\xrightarrow{\delta}\widehat{\mathbf{H}}^2(G,A)\xrightarrow{(x\cup\cdot)^{-1}}\widehat{\mathbf{H}}^0(G,A).$$

Call the composed map ϕ. Then the following diagram is exact (i.e., the kernel of each arrow is the image of the previous one):



The statement easily follows. □

Proposition 1.17.7. *If a G-module A has finite cardinality, then $h(A)=1$.*

Proof. First note that $h(A)$ is defined since all $\widehat{\mathbf{H}}^i(G,A)$ are finite. Let $s\in G$ be a generator. We have exact sequences

$$0\to A^G\to A\xrightarrow{1-[s]}A\to A_G\to 0$$

and

$$0\to\widehat{\mathbf{H}}^{-1}(G,A)\to A_G\xrightarrow{\mathrm{N}_G}A^G\to\widehat{\mathbf{H}}^0(G,A)\to 0.$$

The first shows that $|A^G|=|A_G|$, and the second shows that $h^0(A)=h^1(A)$. □

1.18. **Tate's theorem.** Let G be a finite group. Our approach to Tate's theorem (Theorem 1.18.5 below) follows [Neu13, §I.7]. See [Mil20, §II.3] for a different approach using splitting modules (which is Tate's original idea in his 1952 paper [Tat52]). See [CF+67, Chap.IV, §§9–10] or [Ser79, §IX] for more refined versions of the theorem, whose proofs are more complicated.

Definition 1.18.1. A G-module A is called *cohomologically trivial*, if $\widehat{\mathbf{H}}^i(H,A)=0$ for all subgroups $H\le G$ and all $i\in\mathbb{Z}$.

Example 1.18.2. Recall that an induced G-module is also induced as an H-module, for any $H\le G$. Hence induced G-modules, and more generally their direct summands (i.e. relatively projective G-modules), are cohomologically trivial.

Theorem 1.18.3. *A G-module A is cohomologically trivial if there exists $q \in \mathbb{Z}$ such that for all subgroups $H \leq G$ we have $\widehat{\mathbf{H}}^q(H, A) = \widehat{\mathbf{H}}^{q+1}(H, A) = 0$.*

Proof. Firstly, observe that we only need to show that

$$\widehat{\mathbf{H}}^{q-1}(G, A) = \widehat{\mathbf{H}}^{q+2}(G, A) = 0,$$

since we can recursively apply this result to conclude that $\widehat{\mathbf{H}}^i(G, A) = 0$ for all i, and then we can also replace G by its subgroups, to conclude the proof.

By dimension shifting we may assume that $q = 1$. (Since an induced G-module is cohomologically trivial, by dimension shifting we can find a G-module $A_\pm$ such that $\widehat{\mathbf{H}}^i(H, A_\pm) \cong \widehat{\mathbf{H}}^{i\pm1}(H, A)$ for all subgroups $H \leq G$ and all $i \in \mathbb{Z}$.)

First assume that G is solvable. Then G admits a proper normal subgroup N such that G/N is cyclic. By induction we may assume that the theorem holds for N. Since A satisfies the same assumptions with G replaced by N, we know that A is cohomologically trivial as an N-module. It follows that for all $i \geq 1$, we have the inflation-restriction exact sequence

$$0 \to \mathbf{H}^i(G/N, A^N) \xrightarrow{\text{Inf}} \mathbf{H}^i(G, A) \xrightarrow{\text{Res}} \mathbf{H}^i(N, A) = 0.$$

Since $\mathbf{H}^i(G, A) = 0$ for $i \in \{1, 2\}$, we have $\mathbf{H}^i(G/N, A^N) = 0$ for $i \in \{1, 2\}$. But G/N is cyclic, so by periodicity-2 we know that $\widehat{\mathbf{H}}^i(G/N, A^N) = 0$ for all $i \in \mathbb{Z}$. By the above exact sequence for $i = 3$, we conclude that $\mathbf{H}^3(G, A) = 0$.

Since $\widehat{\mathbf{H}}^0(G/N, A^N) = \widehat{\mathbf{H}}^0(N, A) = 0$, we have

$$A^G = (A^N)^{G/N} = \mathrm{N}_{G/N}(A^N) = \mathrm{N}_{G/N}(\mathrm{N}_N A) = \mathrm{N}_G(A).$$

Hence $\widehat{\mathbf{H}}^0(G, A) = 0$. The proof of the theorem is complete for G solvable.

For general G, let p be a prime dividing $|G|$ and let G_p be a Sylow p-subgroup. Since G_p is solvable, we have $\widehat{\mathbf{H}}^i(G_p, A) = 0$ for all $i \in \mathbb{Z}$ by the above. Since $\mathrm{Cor}_{G/G_p} \circ \mathrm{Res}_{G/G_p} = [G : G_p]$, it follows that $\widehat{\mathbf{H}}^i(G, A)$ is killed by $[G : G_p]$. Hence it is killed by the greatest common divisor of $[G : G_p]$ for all p, which is 1. □

Lemma 1.18.4. *Let A, B be G-modules, and let $\alpha \in \widehat{\mathbf{H}}^0(G, A)$. Let $a \in A^G$ be a lift of α. Then for each $i \in \mathbb{Z}$, the map $\alpha \cup \cdot : \widehat{\mathbf{H}}^i(G, B) \to \widehat{\mathbf{H}}^i(G, A \otimes B)$ is the same as the functorial map induced by the G-homomorphism $B \to A \otimes B, b \mapsto a \otimes b$. (Note that the last map is indeed a G-homomorphism since a is G-invariant.)*

Proof. By dimension shifting (cf. the proof of Lemma 1.17.1) we easily reduce to the case $i = 0$, when the lemma is clear. □

Theorem 1.18.5 (Tate)**.** *Let A be a G-module. Let $q \in \mathbb{Z}$ be such that for each subgroup $H \leq G$, we have $\widehat{\mathbf{H}}^{q-1}(H, A) = 0$ and $\widehat{\mathbf{H}}^q(H, A) \cong \mathbb{Z}/|H|$. Then any generator α of $\widehat{\mathbf{H}}^q(G, A) \cong \mathbb{Z}/|G|$ has the property that the map*

$$\mathrm{Res}(\alpha) \cup \cdot : \widehat{\mathbf{H}}^i(H, \mathbb{Z}) \longrightarrow \widehat{\mathbf{H}}^{i+q}(H, A)$$

is an isomorphism for each $H \leq G$ and each $i \in \mathbb{Z}$. Here Res *denotes the restriction $\widehat{\mathbf{H}}^q(G, A) \to \widehat{\mathbf{H}}^q(H, A)$.*

Remark 1.18.6. The assumptions in the theorem are clearly necessary for the conclusion, since we always have $\widehat{\mathbf{H}}^0(H, \mathbb{Z}) \cong \mathbb{Z}/|H|$ and $\widehat{\mathbf{H}}^{-1}(H, \mathbb{Z}) = 0$.

Proof. We first observe that for any subgroup $H \leq G$, the element $\mathrm{Res}(\alpha) \in \widehat{\mathbf{H}}^q(H, A) \cong \mathbb{Z}/|H|$ is a generator. Indeed, if its order is less than $|H|$, then $\mathrm{Cor} \circ \mathrm{Res}(\alpha) = [G : H]\alpha$ has order less than $|H|$, contradicting with the assumption that α generates $\widehat{\mathbf{H}}^p(G, A) \cong \mathbb{Z}/|G|$. Thus the pair $(H, \mathrm{Res}\,\alpha)$ satisfies the same hypothesis as (G, α), and so we only need to prove that

$$\alpha \cup \cdot : \widehat{\mathbf{H}}^i(G, \mathbb{Z}) \longrightarrow \widehat{\mathbf{H}}^{i+q}(G, A)$$

is an isomorphism for each $i \in \mathbb{Z}$.

Now to prove this statement, by dimension shifting we reduce to the case $q = 0$. Let $a \in A^G$ be a lift of α. By Lemma 1.18.4, we only need to show that the G-homomorphism

$$f : \mathbb{Z} \longrightarrow A, \quad n \longmapsto na$$

induces isomorphisms $\widehat{\mathbf{H}}^i(G, \mathbb{Z}) \xrightarrow{\sim} \widehat{\mathbf{H}}^i(G, A)$ for all $i \in \mathbb{Z}$. Up to replacing A by $A \oplus \mathbb{Z}[G]$ and replacing a by $a \oplus \sum_{g \in G}[g]$, which does not change Tate cohomology at all since $\mathbb{Z}[G]$ is induced, we may assume that f is injective. (This is the key trick, taken from the proof of [Neu13, §I, Thm. 7.2].) Let $A' = \mathrm{Cok}(f)$. Then we only need to show that A' is cohomologically trivial as a G-module. Let $H \leq G$. Since $\widehat{\mathbf{H}}^{-1}(H, A) = 0$ by assumption and $\widehat{\mathbf{H}}^1(H, \mathbb{Z}) = \mathrm{Hom}_{\mathrm{gp}}(H, \mathbb{Z}) = 0$, we have an exact sequence

$$0 \to \widehat{\mathbf{H}}^{-1}(H, A') \to \widehat{\mathbf{H}}^0(H, \mathbb{Z}) \xrightarrow{(*)} \widehat{\mathbf{H}}^0(H, A) \to \widehat{\mathbf{H}}^0(H, A') \to 0,$$

where $(*)$ is the functorial map induced by f. If we can show that (*) is an isomorphism, then $\widehat{\mathbf{H}}^{-1}(H, A') = \widehat{\mathbf{H}}^0(H, A') = 0$, and so A' is cohomologically trivial by Theorem 1.18.3 since H is arbitrary. But (*) is an isomorphism since it sends $1 \in \widehat{\mathbf{H}}^0(H, \mathbb{Z}) = \mathbb{Z}/|H|$ to the image of a in $\widehat{\mathbf{H}}^0(H, A) = A^H/\mathrm{N}_H(A)$, which is a generator of $\widehat{\mathbf{H}}^0(H, A) \cong \mathbb{Z}/|H|$ by our first observation. □

We shall apply Theorem 1.18.5 to the following situation. Let L/K be a finite Galois extension of local fields. Let $G = \mathrm{Gal}(L/K)$. Consider the G-module $A = L^\times$ and the integer $q = 2$. By Galois theory, the hypotheses of the theorem are translated to the following:

Theorem 1.18.7. *For every subextension K'/K inside L, we have $\mathbf{H}^1(\mathrm{Gal}(L/K'), L^\times) = 0$ and $\mathbf{H}^2(\mathrm{Gal}(L/K'), L^\times)$ is cyclic of order $[L : K']$.*

We now study $\mathbf{H}^1$ and $\mathbf{H}^2$ in the above theorem. We may assume $K' = K$ since the desired statements depend only on the extension L/K'.

1.19. **Hilbert's Theorem 90 and consequences.** Let L/K be a finite Galois extension of fields, and let $G = \mathrm{Gal}(L/K)$. The groups $(L, +)$ and $(L^\times, \times)$ are G-modules.

Proposition 1.19.1. *We have $\widehat{\mathbf{H}}^i(G, L) = 0$ for all $i \in \mathbb{Z}$.*

Proof. By the normal basis theorem, $L \cong \mathrm{Ind}_1^G K$ is an induced G-module. □

Theorem 1.19.2 (Hilbert's Theorem 90)**.** *We have $\mathbf{H}^1(G, L^\times) = 0$.*

Proof. Let ϕ be a 1-cocycle in $C^1(G, L^\times)$. Recall that this means ϕ is a function $G \to L^\times, s \mapsto \phi_s$ satisfying $\phi_{st} = \phi_s \cdot s(\phi_t)$. We need to show that ϕ is a coboundary, i.e., $\phi_s = b/s(b)$ for some fixed $b \in L^\times$.

Let $a \in L^\times$, and let

$$b := \sum_{t \in G} \phi_t \cdot t(a) \in L.$$

By the linear independence of the characters $t : L^\times \to L^\times$ (where t runs through G), we can find a such that $b \neq 0$. For $s \in G$, we compute

$$s(b) = \sum_{t\in G} s(\phi_t)\cdot(st)(a) = \sum_{t\in G} \frac{\phi_{st}}{\phi_s}\cdot(st)(a) = \phi_s^{-1}b.$$

Thus $\phi_s = b/s(b)$ as desired. □

Corollary 1.19.3 (Original Hilbert's Theorem 90)**.** *Assume that L/K is a cyclic extension. Let $s \in G$ be a generator. Then any element of L whose norm to K is 1 can be written as $s(a)/a$ for some $a \in L^\times$.*

Proof. Since G is cyclic, we have $\widehat{\mathbf{H}}^{-1}(G, L^\times) \cong \widehat{\mathbf{H}}^1(G, L^\times) = 0$. But $\widehat{\mathbf{H}}^{-1}(G, L^\times)$ is the quotient of $\ker(\mathrm{N}_{L/K} : L^\times \to K^\times)$ by $I_G \cdot L^\times = \{s(a)/a \mid a \in L^\times\}$. □

Corollary 1.19.4. *If K is a finite field , then $\widehat{\mathbf{H}}^i(G, L^\times) = 0$ for all $i \in \mathbb{Z}$. In particular, $\mathrm{N}_{L/K} : L^\times \to K^\times$ is surjective.*

Proof. In this case G is cyclic, and the Herbrand quotient $h(L^\times) = 1$ since $L^\times$ is finite. Thus the vanishing of $\widehat{\mathbf{H}}^1(G, L^\times)$ implies the vanishing of all $\widehat{\mathbf{H}}^i(G, L^\times)$. The "in particular" part follows from the vanishing of $\widehat{\mathbf{H}}^0(G, L^\times)$. □

Exercise 1.19.5. Let L/K be a finite extension of finite fields. Use elementary methods to show that $\mathrm{N}_{L/K} : L^\times \to K^\times$ is surjective.

1.20. **Brauer groups.** Let K be a field. Let L/K and E/K be finite Galois extensions, with $E \subset L$. Write $G_{L/K}$ for $\mathrm{Gal}(L/K)$, etc. We have $G_{E/K} = G_{L/K}/G_{L/E}$, and $E^\times = (L^\times)^{G_{L/E}}$. Thus for $q \geq 1$ we have the inflation-restriction sequence

$$0 \to \mathbf{H}^q(G_{E/K}, E^\times) \xrightarrow{\mathrm{Inf}} \mathbf{H}^q(G_{L/K}, L^\times) \xrightarrow{\mathrm{Res}} \mathbf{H}^q(G_{L/E}, L^\times).$$

Recall that this sequence is exact if $\mathbf{H}^i(G_{L/E}, L^\times) = 0$ for all $1 \leq i \leq q-1$ (see Proposition 1.12.2). Since $\mathbf{H}^1(G_{L/E}, L^\times) = 0$, the above sequence is exact for $q = 2$.

Definition 1.20.1. The *Brauer group* for the finite Galois extension L/K is $\mathrm{Br}(L/K) := \mathbf{H}^2(G_{L/K}, L^\times)$.

Thus we have an exact sequence

$$0 \to \mathrm{Br}(E/K) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(L/K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(L/E).$$

We shall regard $\mathrm{Inf} : \mathrm{Br}(E/K) \to \mathrm{Br}(L/K)$ as inclusion.

Definition 1.20.2. The *absolute Brauer group of K* is $\mathrm{Br}(K) := \bigcup_L \mathrm{Br}(L/K)$ where L runs thourgh all finite Galois extensions of K inside K^s. In other words, $\mathrm{Br}(K)$ is the direct limit of $\mathrm{Br}(L/K)$, where the transition maps are the injections $\mathrm{Inf} : \mathrm{Br}(L/K) \to \mathrm{Br}(L'/K)$ when $L \subset L'$.

Note that for three finite Galois extensions E, L, L' of K with $E \subset L \subset L'$, the following diagram commutes:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Br}(E/K) & \xrightarrow{\mathrm{Inf}} & \mathrm{Br}(L/K) & \xrightarrow{\mathrm{Res}} & \mathrm{Br}(L/E) \\
 & & \| & & \downarrow{\scriptstyle \mathrm{Inf}} & & \downarrow{\scriptstyle \mathrm{Inf}} \\
0 & \longrightarrow & \mathrm{Br}(E/K) & \xrightarrow{\mathrm{Inf}} & \mathrm{Br}(L'/K) & \xrightarrow{\mathrm{Res}} & \mathrm{Br}(L'/E)
\end{array}$$

(The commutativity follows easily from the cochain descriptions of Inf and Res.) Thus by fixing E and taking the direct limit over L we have an exact sequence

$$0 \to \mathrm{Br}(E/K) \xrightarrow{\mathrm{Inf}} \mathrm{Br}(K) \xrightarrow{\mathrm{Res}} \mathrm{Br}(E).$$

The first map is of course nothing but the "inclusion" in the sense that $\mathrm{Br}(E/K)$ is a member of the direct limit/union defining $\mathrm{Br}(K)$. Slightly more generally, if E/K is any finite extension, then we still have the right square in the above commutative diagram, and so we have a well-define map $\mathrm{Res} : \mathrm{Br}(K) \to \mathrm{Br}(E)$.

Example 1.20.3. If K is a finite field, then $\mathrm{Br}(K) = 0$ by Corollary 1.19.4.

Remark 1.20.4. It turns out that $\mathrm{Br}(K)$ can be identified with the *classical Brauer group* of K. This is the set of equivalence classes of central simple algebras over K. Two central simple algebras A and B over K are equivalent if and only if $A \cong M_n(D)$ and $B \cong M_m(D)$ for some integers n, m and a central division algebra D over K. (Here n and D are uniquely determined by A.) The group operation is given by $\otimes_K$. The subgroup $\mathrm{Br}(E/K) \subset \mathrm{Br}(K)$ is identified with the subgroup of the equivalence classes of central simple algebras over K which split over E (i.e., those A such that $A \otimes_K E \cong M_n(E)$). The map $\mathrm{Res} : \mathrm{Br}(K) \to \mathrm{Br}(E)$ is given by base changing the central simple algebras from K to E. The identification is given by an explicit construction, namely, starting with a 2-cocycle in $Z^2(G_{E/K}, E^\times)$ one can explicitly write down a central simple algebra over K which splits over E. For details see [Ser79, §X.5] and [Mil20, §IV]. We will not need this relationship in our course.

Remark 1.20.5. By Wedderburn's Little Theorem, every finite division ring is a field. This shows that the classical Brauer group of a finite field vanishes. Compare with Example 1.20.3.

In order to finish the proof of Theorem 1.18.7, we need to show that when L/K is a finite Galois extension of local fields we have $\mathrm{Br}(L/K) \cong \mathbb{Z}/[L : K]$.

1.21. **The Brauer group of an unramified extension.** Let L/K be an unramified extension of local fields of degree n. We shall compute $\mathrm{Br}(E/K)$. Let $G = \mathrm{Gal}(L/K)$, and let $U = \mathcal{O}_L^\times$. We have a short exact sequence of G-modules

$$1 \to U \to L^\times \xrightarrow{v} \mathbb{Z} \to 0,$$

where v is the valuation.

Proposition 1.21.1. *For all $q \in \mathbb{Z}$, the valuation $v : L^\times \to \mathbb{Z}$ induces an isomorphism $\widehat{\mathbf{H}}^q(G, L^\times) \xrightarrow{\sim} \widehat{\mathbf{H}}^q(G, \mathbb{Z})$, and $\widehat{\mathbf{H}}^q(G, U) = 0$.*

The proof uses the following lemma.

Lemma 1.21.2. *Let G be a finite group and U a G-module. Assume that there is a decreasing sequence of G-submodules $U = U^0 \supset U^1 \supset U^2 \supset \cdots$ such that the natural map $U \to \varprojlim_i U/U_i$ is an isomorphism. If $q \in \mathbb{Z}$ is such that $\widehat{\mathbf{H}}^q(G, U^i/U^{i+1}) = 0$ for all $i \geq 0$, then we have $\widehat{\mathbf{H}}^q(G, U) = 0$.*

Proof. Let $(P_\bullet)_{\bullet \in \mathbb{Z}}$ be a complete resolution of $\mathbb{Z}$, and we use it to compute Tate cohomology. Thus for any G-module X, $\widehat{\mathbf{H}}^q(G, X)$ is the q-th cohomology of $(\mathrm{Hom}_{\mathbb{Z}[G]}(P_\bullet, X))$. Write $C^q(X)$ for $\mathrm{Hom}_{\mathbb{Z}[G]}(P_q, X)$. This is identified with the group of all maps $G^{n_q} \to X$ for some $n_q \geq 0$. (For instance, if $P_\bullet$ arises from the standard free resolution in Proposition 1.7.1, then $P_q = \mathbb{Z}[G]^{q+1}$ for $q \geq 0$ and $P_q = \mathbb{Z}[G]^{-q}$ for $q \leq -1$. Thus $n_q = q$ for $q \geq 0$ and $n_q = -q - 1$ for $q \leq -1$.)

Write d for all the differential maps in $C^\bullet(\cdot)$. Let $f \in C^q(U)$ be such that $df = 0$. We need to find $h \in C^{q-1}(U)$ such that $dh = f$. Write $\bar{f}$ for the image of f in $C^q(U/U^1)$. Then $d\bar{f} = 0$. Since $\widehat{\mathbf{H}}^q(G, U/U^1) = 0$, there exists $\bar{h}_0 \in C^{q-1}(U/U^1)$ such that $\bar{f} = d\bar{h}_0$. Let $h_0 \in C^{q-1}(U)$ be a lift of $\bar{h}_0$. Then $f - dh_0 \in C^q(U)$ is a map $G^{n_q} \to U$ whose image lies in U^1, i.e., $f - dh_0 \in C^q(U^1)$. Similarly, we find $h_i \in C^{q-1}(U^i)$ for all $i \geq 0$ such that $f - dh_0 - dh_1 - \cdots - dh_i \in C^1(U^{i+1})$. Let $h = h_0 + h_1 + \cdots \in U \cong \varprojlim_i U/U^i$, i.e., it is the element whose projection in U/U^i is $h_0 + h_1 + \cdots + h_{i-1}$. Then $f - dh \in C^q(U)$ is a map $G^{n_q} \to U$ whose image lies in U^i for all i, which implies that $f = dh$. □

Proof of Proposition 1.21.1. It suffices to prove the second statement. Let $U^0 = U$ and $U^i = 1 + \mathfrak{m}_L^i$ for $i \geq 1$. Since U is profinite and $\{U^i\}$ is a neighborhood basis of 1, the natural map $U \to \varprojlim_i U/U^i$ is an isomorphism. Thus by Lemma 1.21.2, it suffices to show $\widehat{\mathbf{H}}^q(G, U^i/U^{i+1})$ for all $i \geq 0$.

For $i = 0$, we have $U^0/U^1 \cong k_L^\times$ (where k_L denotes the residue field of L), and the isomorphism is G-equivariant. We have $\widehat{\mathbf{H}}^q(G, k_L^\times) = \widehat{\mathbf{H}}^q(\mathrm{Gal}(k_L/k_K), k_L^\times)$ (here $G \cong \mathrm{Gal}(k_L/k_K)$), and we have seen the vanishing of this in Corollary 1.19.4.

For $i \geq 1$, we have a G-equivariant isomorphism $(k_L, +) \xrightarrow{\sim} U^i/U^{i+1}$ induced by $\mathcal{O}_L \to U^i, x \mapsto 1 + \pi^i x$ where π is a uniformizer in K. We have seen the vanishing of $\widehat{\mathbf{H}}^q(\mathrm{Gal}(k_L/k_K), k_L)$ in Proposition 1.19.1. □

Theorem 1.21.3. *We have a canonical isomorphism* $\mathrm{inv} : \mathrm{Br}(L/K) \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

Proof. By Proposition 1.21.1, we have a canonical isomorphism $\mathrm{Br}(L/K) \cong \mathbf{H}^2(G, \mathbb{Z})$. Now G acts trivially on $\mathbb{Z}$, and we have a short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. We have $\widehat{\mathbf{H}}^i(G, \mathbb{Q}) = 0$ since on the one hand this is killed by $|G|$ and on the other hand multiplication by $|G|$ must be an automorphism since it is an automorphism on $\mathbb{Q}$.[2] Therefore the connecting homomorphism gives an isomorphism

$$\delta : \mathbf{H}^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \mathbf{H}^2(G, \mathbb{Z}).$$

The left hand side is just $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$, and this is canonically isomorphic to $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ by looking at where the Frobenius generator $\sigma \in G \cong \mathbb{Z}/n\mathbb{Z}$ goes to. In other words, we have $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z}, f \mapsto f(\sigma)$. □

Remark 1.21.4. Using that $\widehat{\mathbf{H}}^0(\mathrm{Gal}(L/K), \mathcal{O}_L^\times) = 0$ and that $(\mathcal{O}_L^\times)^{\mathrm{Gal}(L/K)} = \mathcal{O}_K^\times$, we get the useful result that the norm map $\mathrm{N}_{L/K} : \mathcal{O}_L^\times \longrightarrow \mathcal{O}_K^\times$ is surjective (for unramified L/K).

1.22. **Functoriality of** inv**.** Let K be a local field. For each $n \geq 1$, let K_n be the unique degree n unramified extension of K inside a fixed separable closure K^s. We have constructed a canonical isomorphism

$$\mathrm{inv} : \mathrm{Br}(K_n/K) \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

If $n|m$, then $K_n \subset K_m$. In this case we have a diagram

$$\begin{array}{ccc} \mathrm{Br}(K_n/K) & \xrightarrow{\mathrm{inv}} & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Inf}} & & \downarrow{\scriptstyle \mathrm{id}} \\ \mathrm{Br}(K_m/K) & \xrightarrow{\mathrm{inv}} & \frac{1}{m}\mathbb{Z}/\mathbb{Z} \end{array}$$

[2] We are using the following simple fact: For a G-module A and an integer n, the functorial endomorphism of $\widehat{\mathbf{H}}^i(G, A)$ induced by $A \to A, a \mapsto na$ is multiplicaiton by n. This can be seen using dimension shifting.

Chasing the constructions (especially using the compatibility of inflation with connecting homomorphisms), we see that the above diagram commutes.

We define $\mathrm{Br}(K^{\mathrm{ur}}/K) := \bigcup_n \mathrm{Br}(K_n/K)$. (This is a subgroup of $\mathrm{Br}(K)$, and we will later see that it is in fact equal to $\mathrm{Br}(K)$.) Then we have a canonical isomorphism

$$\mathrm{inv} : \mathrm{Br}(K^{\mathrm{ur}}/K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

We now let L/K be a possibly ramified finite separable extension inside K^s. For each $n \geq 1$, we form the compositum LK_n inside K^s. Then the extension LK_n/L is finite unramified (but its degree may be less than n). Thus we have

$$\mathrm{inv} : \mathrm{Br}(LK_n/L) \hookrightarrow \mathbb{Q}/\mathbb{Z}.$$

We view $\mathrm{Gal}(LK_n/L)$ as a subgroup of $\mathrm{Gal}(K_n/K)$ via $\mathrm{Gal}(LK_n/L) \hookrightarrow \mathrm{Gal}(K_n/K), \tau \mapsto \tau|_{K_n}$. We denote the composite map

$$\begin{aligned}\mathrm{Br}(K_n/K) = \mathbf{H}^2(\mathrm{Gal}(K_n/K), K_n^\times) &\xrightarrow{\mathrm{Res}} \mathbf{H}^2(\mathrm{Gal}(LK_n/L), K_n^\times) \\ &\to \mathbf{H}^2(\mathrm{Gal}(LK_n/L), (LK_n)^\times) = \mathrm{Br}(LK_n/L)\end{aligned}$$

still by Res.

Lemma 1.22.1. *The diagram*

$$\begin{array}{ccc} \mathrm{Br}(K_n/K) & \xrightarrow{\mathrm{Res}} & \mathrm{Br}(LK_n/L) \\ \downarrow{\scriptstyle \mathrm{inv}} & & \downarrow{\scriptstyle \mathrm{inv}} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:K]} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes.

Proof. Let $e = e(L/K)$ and $f = f(L/K)$. We have a commutative diagram

$$\begin{array}{ccccccc} \mathrm{Br}(K_n/K) & \xrightarrow[\cong]{v_K} & \mathbf{H}^2(G_{K_n/K}, \mathbb{Z}) & \xleftarrow[\cong]{\delta} & \mathbf{H}^1(G_{K_n/K}, \mathbb{Q}/\mathbb{Z}) & \hookrightarrow & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle e\cdot\mathrm{Res}} & & \downarrow{\scriptstyle e\cdot\mathrm{Res}} & & \downarrow{\scriptstyle ef} \\ \mathrm{Br}(LK_n/L) & \xrightarrow[\cong]{v_L} & \mathbf{H}^2(G_{LK_n/L}, \mathbb{Z}) & \xleftarrow[\cong]{\delta} & \mathbf{H}^1(G_{LK_n/L}, \mathbb{Q}/\mathbb{Z}) & \hookrightarrow & \mathbb{Q}/\mathbb{Z} \end{array}$$

and the two rows define inv in the two cases. The first square commutes becasue $v_K = e \cdot v_L|_{K^\times}$. The second square commutes because Res is compatible with the connecting homomorphisms attached to $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. The third diagram commutes because the Frobenius generator in $\mathrm{Gal}(K_n/K)$ is the f-th power of the image of the Frobenius in $\mathrm{Gal}(LK_n/L)$ under the map $\mathrm{Gal}(LK_n/L) \to \mathrm{Gal}(K_n/K)$. (To see this, note that the images of the two Frobenius elements in $\mathrm{Aut}(k_{K_n})$ are the automorphisms $x \mapsto x^{|k_K|}$ and $x \mapsto x^{|k_L|}$ respectively, and $|k_L| = |k_K|^f$.) □

Taking direct limit over n, we obtain:

Proposition 1.22.2. *We have a commutative diagram*

$$\begin{array}{ccc} \mathrm{Br}(K^{\mathrm{ur}}/K) & \xrightarrow{\mathrm{Res}} & \mathrm{Br}(L^{\mathrm{ur}}/L) \\ \cong\downarrow{\scriptstyle \mathrm{inv}} & & \cong\downarrow{\scriptstyle \mathrm{inv}} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:K]} & \mathbb{Q}/\mathbb{Z} \end{array}$$

Thus the kernel Φ of the first row is cyclic of order $[L : K]$. Note that if L/K is finite Galois, then Φ is a subgroup of $\mathrm{Br}(L/K)$, since $\mathrm{Br}(L/K) \subset \mathrm{Br}(K)$ is the kernel of $\mathrm{Res} : \mathrm{Br}(K) \to \mathrm{Br}(L)$. Thus we have proved:

Lemma 1.22.3. *Let L/K be a degree n finite Galois extension. Let $\Phi = \mathrm{inv}^{-1}(\frac{1}{n}\mathbb{Z}/\mathbb{Z}) \subset \mathrm{Br}(K^{\mathrm{ur}}/K)$. Then Φ is contained in $\mathrm{Br}(L/K)$ (where both are viewed as subgroups of $\mathrm{Br}(K)$).* □

Our next goal is to show that the containment in the above lemma is in fact an equality. For this, it suffices to show the following result.

Theorem 1.22.4 (Upper bound for the Brauer group)**.** *The order of $\mathrm{Br}(L/K)$ divides $[L : K]$.*

Corollary 1.22.5. *For every degree n Galois extension L/K, $\mathrm{Br}(L/K)$ is equal to $\mathrm{Br}(K_n/K)$ as a subgroup of $\mathrm{Br}(K)$. In particular, there is a canonical isomorphism $\mathrm{inv} : \mathrm{Br}(L/K) \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. We also have $\mathrm{Br}(K) = \mathrm{Br}(K^{\mathrm{ur}}/K)$, and there is a canonical isomorphism $\mathrm{inv} : \mathrm{Br}(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$.* □

Remark 1.22.6. In the classical language, the above result says that every central simple algebra over K splits over a finite *unramified* extension of K. Moreover, the equivalence classes of central simple algebras are classified by an invariant in $\mathbb{Q}/\mathbb{Z}$.

At this point, we have proved Theorem 1.18.7, modulo proving Theorem 1.22.4.

1.23. **Proof of the upper bound.** We now prove Theorem 1.22.4. Our approach follows [CF+67, §VI.1.4-VI.1.6] with slight simplifications.

Let L/K be a degree n Galois extension of local fields. Let $G = \mathrm{Gal}(L/K)$ and $U = \mathcal{O}_L^\times$. Let π be a uniformizer in K.

Lemma 1.23.1. *There exists a G-stable open subgroup V of U such that $\widehat{\mathbf{H}}^q(G, V) = 0$ for all $q \in \mathbb{Z}$.*

Proof. Let $\{e_1, \cdots, e_n\}$ be a normal basis for L/K, that is, it is a K-basis of L, and G permutes the e_i's simply transitively. Let $A = \mathcal{O}_K e_1 \oplus \cdots \oplus \mathcal{O}_K e_n \subset L$. Up to replacing e_i by $\pi^r e_i$ for a large integer r (common for all i), we may assume that each e_i lies in $\mathcal{O}_L$, and in particular $A \subset \mathcal{O}_L$. Note that A is open, since the topology on $L \cong K^n$ is just the product topology of the topology on K. Therefore there exists $N \geq 1$ such that $A \supset \pi^N \mathcal{O}_L$.

Let $M = \pi^{N+1}A$. We claim that $M \cdot M \subset \pi M$. Indeed,

$$M \cdot M = \pi^{2N+2} A \cdot A \subset \pi^{2N+2}\mathcal{O}_L = \pi^{N+2}\pi^N \mathcal{O}_L \subset \pi^{N+2} A = \pi M.$$

Let $V = 1 + M$. We claim that V is an open, G-stable subgroup of U. To see that V is closed under multiplication, use that $M + M \subset M$ and $M \cdot M \subset \pi M \subset M$. To see that V is closed under inversion, use that $(1-m)^{-1} = 1 + \sum_{k\geq 1} m^k$ for all $m \in \mathfrak{m}_L$ (and in particular for all $m \in M$). For $m \in M$, the sum of the converging series $\sum_{k\geq 1} m^k$ lies in M since M is an open and hence closed subgroup of $\mathcal{O}_L$. Thus V is a subgroup of U. Since A is open in L, so is M, and hence V is open in L. Thus V is an open subgroup of U. Finally, V is stable under G since G fixes π and stabilizes A.

It remains to show that $\widehat{\mathbf{H}}^q(G, V) = 0$ for all $q \in \mathbb{Z}$. We have a decreasing filtration

$$V = V^0 \supset V^1 \supset V^2 \supset \cdots$$

where $V^i = 1 + \pi^i M \subset V$. Since V is profinite (being an open subgroup of U) and $\{V^i\}$ is clearly a neighborhood basis of 1, the natural map $V \to \varprojlim_i V/V^i$ is an isomorphism.

Moreover each V^j is G-stable. Thus by Lemma 1.21.2, the vanishing of $\widehat{\mathbf{H}}^q(G,V)$ follows from the vanishing of $\widehat{\mathbf{H}}^q(G,V^i/V^{i+1})$ for all $i\geq 0$. We have a G-module isomorphism $M/\pi M\xrightarrow{\sim} V^i/V^{i+1}, m\mapsto 1+\pi^i m$. Indeed, this map is clearly a G-module isomorphism once we know it is a group homomorphism. To check that it is a group homomorphism, we have

$$(1+\pi^i m_1)(1+\pi^i m_2)=1+\pi^i(m_1+m_2)+\pi^{2i}m_1m_2=(1+\pi^i(m_1+m_2))(1+\frac{\pi^{2i}m_1m_2}{1+\pi^i(m_1+m_2)}).$$

We need to check that

$$1+\frac{\pi^{2i}m_1m_2}{1+\pi^i(m_1+m_2)}\in V^{i+1}.$$

We have

$$1+\frac{\pi^{2i}m_1m_2}{1+\pi^i(m_1+m_2)}=1+\pi^{2i}m_1m_2\sum_{j=0}^{\infty}(-1)^j\pi^{ij}(m_1+m_2)^j.$$

The infinite sum lies in $1+M$, so the above lies in

$$1+\pi^{2i}M\cdot M(1+M)\subset 1+\pi^{2i+1}M(1+M)\subset 1+\pi^{2i+1}M+\pi^{2i+2}M\subset 1+\pi^{2i+1}M\subset V^{i+1},$$

as desired.

Now $M/\pi M\cong A/\pi A\cong k_Ke_1\oplus\cdots\oplus k_Ke_n\cong\mathbb{Z}[G]\otimes_{\mathbb{Z}}k_K$ is induced as a G-module (since $\{e_i\}$ is a normal basis). Hence $\widehat{\mathbf{H}}^q(G,V^i/V^{i+1})=0$ as desired. □

Proof of Theorem 1.22.4. Let $G=\mathrm{Gal}(L/K)$, $n=[L:K]$.

First assume that L/K is cyclic. Let $U=\mathcal{O}_L^\times$, and let $V\subset U$ be as in Lemma 1.23.1. Then the Herbrand quotient $h(V)=1$, and $h(U/V)=1$ because U/V is finite (since V is an open subgroup of the compact U). Thus we have $h(U)=h(V)h(U/V)=1$. Since $L^\times/U\cong\mathbb{Z}$, we have $h(L^\times)=h(U)h(\mathbb{Z})=h(\mathbb{Z})$. We compute that $\widehat{\mathbf{H}}^0(G,\mathbb{Z})=\mathbb{Z}/n$ and $\widehat{\mathbf{H}}^{-1}(G,\mathbb{Z})=0$. Hence $h(\mathbb{Z})=n$. This shows that $h(L^\times)=n$. But $\mathbf{H}^1(G,L^\times)=0$ by Hilbert 90. Hence $\mathrm{Br}(L/K)$ has order n.

For a general L/K, since $\mathrm{Br}(L/K)\cong\widehat{\mathbf{H}}^2(G,L^\times/V)$ is an abelian group killed by n, it suffices to show that for each prime p dividing n, the cardinality of the p-primary part[3] of $\mathrm{Br}(L/K)$ is finite and divides the p-part of n. Let G_p be a Sylow p-subgroup of G, and let $K'=L^{G_p}$. Since the composition $\widehat{\mathbf{H}}^2(G,L^\times)\xrightarrow{\mathrm{Res}}\widehat{\mathbf{H}}^2(G_p,L^\times)\xrightarrow{\mathrm{Cor}}\widehat{\mathbf{H}}^2(G,L^\times)$ is multiplication by $[G:G_p]$ which is coprime to p, the map $\mathrm{Res}:\mathrm{Br}(L/K)\to\mathrm{Br}(L/K')$ is injective on the p-primary part. Thus it suffices to prove the theorem for the extension L/K' instead of L/K.

Hence we may assume that G is a p-group, and in particular solvable.[4] Let $H\leq G$ be a proper normal subgroup such that G/H is cyclic. Let $E=L^H$. By induction on the degree we may assume that the theorem holds for L/E. Also the theorem holds for E/K as we already proved the cyclic case. Now we have the exact sequence

$$0\to\mathrm{Br}(E/K)\xrightarrow{\mathrm{Inf}}\mathrm{Br}(L/K)\xrightarrow{\mathrm{Res}}\mathrm{Br}(L/E).$$

Thus $|\mathrm{Br}(L/K)|$ divides $|\mathrm{Br}(E/K)|\cdot|\mathrm{Br}(L/E)|$, which divides $[E:K][L:E]=[L:K]$. □

[3] By the Chinese Remainder Theorem, if $n=p_1^{e_1}\cdots p_r^{e_r}$ then each $\mathbb{Z}/n$-module M has a canonical primary decomposition $M=\bigoplus_i M_i$ where M_i is a $\mathbb{Z}/p_i^{e_i}$-module.

[4] Every finite extension of a local field is automatically solvable, so this reduction step is actually redundant. However, in the proof we do not need to use this fact, and also the similar reduction argument will be used again in the global case, cf. the discussion below Theorem 2.4.1.

1.24. **The local Artin map.** At this point, we have verified the axioms in Tate's theorem in the setting of a finite Galois extension of local fields, i.e., we have proved Theorem 1.18.7. We summarize the results as follows:

Theorem 1.24.1. *Let L/K be a degree n Galois extension of local fields. Then* $\mathrm{Br}(L/K) = \mathrm{Br}(K_n/K)$ *as subgroups of* $\mathrm{Br}(K)$*, and we have a canonical isomorphism*

$$\mathrm{inv} : \mathrm{Br}(L/K) = \mathrm{Br}(K_n/K) \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

Define

$$u_{L/K} := \mathrm{inv}^{-1}(\frac{1}{n}) \in \mathrm{Br}(L/K),$$

called the fundamental class*. By Tate's theorem, the map*

$$u_{L/K} \cup \cdot : \widehat{\mathbf{H}}^q(\mathrm{Gal}(L/K), \mathbb{Z}) \longrightarrow \widehat{\mathbf{H}}^{q+2}(\mathrm{Gal}(L/K), L^\times)$$

is an isomorphism for each $q \in \mathbb{Z}$. □

Taking $q = -2$ we have the isomorphism

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} \cong \widehat{\mathbf{H}}^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) \xrightarrow{\sim} \widehat{\mathbf{H}}^0(\mathrm{Gal}(L/K), L^\times) = K^\times/\mathrm{N}_{L/K}(L^\times).$$

We denote the inverse isomorphism by $\psi_{L/K}$, and call it the local Artin map. Sometimes we also think of $\psi_{L/K}$ as a surjective homomorphism $K^\times \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$ whose kernel is $\mathrm{N}_{L/K}(L^\times)$.

Lemma 1.24.2. *Let G be a finite group, and let B be a G-module. Let $g \in G$ and $\beta \in Z^1(G, B)$ (a 1-cocycle $\beta : G \to B$). Let $\bar{g}$ be the image of g in $G^{\mathrm{ab}} = \widehat{\mathbf{H}}^{-2}(G, \mathbb{Z})$, and let $\bar{\beta}$ be the image of β in $\widehat{\mathbf{H}}^1(G, B)$. Then the element $\bar{g} \cup \bar{\beta} \in \widehat{\mathbf{H}}^{-1}(G, B) = B[\mathrm{N}_G]/I_G B$ is represented by $\beta(g) \in B$.*[5]

Proof. See [Ser79, App. to Chap. XI, Lem. 3] or [Neu13, I.5.7]. □

Lemma 1.24.3. *Let L/K be a finite Galois extension of local fields with Galois group G. Let $f \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = \widehat{\mathbf{H}}^1(G, \mathbb{Q}/\mathbb{Z})$, and let $a \in K^\times$. Note that f factors through G^{ab}, so $f(\psi_{L/K}(a)) \in \mathbb{Q}/\mathbb{Z}$ is well defined. We have*

$$f(\psi_{L/K}(a)) = \mathrm{inv}(\bar{a} \cup \delta f),$$

where δf is the image of f in $\widehat{\mathbf{H}}^2(G, \mathbb{Z})$ under the connecting homomorphism associated with $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$, and $\bar{a} \in \widehat{\mathbf{H}}^0(G, L^\times) = K^\times/\mathrm{N}(L^\times)$ is the image of a.

Exercise 1.24.4. For any finite abelian group G, define the *Pontryagin dual group* $G^\vee := \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$, where the group operation is point-wise addition. Show that

$$G^\vee \cong \mathrm{Hom}(G, \mathbb{C}^\times) \cong \mathrm{Hom}(G, S^1)$$

(where $S^1 = \{z \in \mathbb{C}^\times \mid |z| = 1\}$), and that $(G^\vee)^\vee$ is canonically isomorphic to G. In particular, two elements $g_1, g_2 \in G$ are equal if and only if for all $f \in G^\vee$ we have $f(g_1) = f(g_2)$.

Remark 1.24.5. Since G^{ab} is a finite abelian group, the element $\psi_{L/K}(a) \in G^{\mathrm{ab}}$ is characterized by the values $f(\psi_{L/K}(a))$ for all f by the above exercise. Hence the above lemma gives a characterization of the map $\psi_{L/K}$.

[5] Note that $\mathrm{N}_G(\beta(g)) = \sum_{h \in G} h(\beta(g)) = \sum_h \beta(hg) - \beta(h) = 0$, so indeed $\beta(g) \in B[\mathrm{N}_G]$.

Proof of Lemma 1.24.3. Write g for $\psi_{L/K}(a) \in \widehat{\mathbf{H}}^{-2}(G,\mathbb{Z})$. Write u for the fundamental class $u_{L/K}$. By the definition of $\psi_{L/K}$, we have

$$\bar{a} = u \cup g \in \widehat{\mathbf{H}}^0(G, L^\times).$$

Thus

$$\bar{a} \cup \delta f = (u \cup g) \cup \delta f = u \cup (g \cup \delta f) = u \cup \delta(g \cup f).$$

Here $g \cup f$ lies in $\widehat{\mathbf{H}}^{-1}(G, \mathbb{Q}/\mathbb{Z})$, and δ of it lies in $\widehat{\mathbf{H}}^0(G,\mathbb{Z})$. Note that $\widehat{\mathbf{H}}^{-1}(G,\mathbb{Q}/\mathbb{Z})$ is the n-torsion of $\mathbb{Q}/\mathbb{Z}$, namely $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. By Lemma 1.24.2, the element $g \cup f \in \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ is equal to $f(g)$. Write $f(g) = r/n \mod \mathbb{Z}$. Then $\delta(g \cup f) = \delta(r/n) \in \widehat{\mathbf{H}}^0(G,\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ is represented by $\mathrm{N}_G(r/n) = n \cdot r/n = r \in \mathbb{Z}$. Thus from the above computation we have

$$\bar{a} \cup \delta f = u \cup \bar{r} = r \cdot u.$$

The inv of this element is $r \cdot \mathrm{inv}(u) = r/n \mod \mathbb{Z}$ (since $\mathrm{inv}(u) = 1/n \mod \mathbb{Z}$), which is equal to $f(g)$ as desired. □

For every finite abelian extension L/K, we have the local Artin map $\psi_{L/K} : K^\times \to \mathrm{Gal}(L/K)$. In order for them to define a continuous homomorphism $K^\times \to G_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$, we need to check the following compatibility:

Lemma 1.24.6. *Let $L' \supset L$ be two finite Galois extensions of K. The following diagram commutes:*

$$\begin{array}{ccc} K^\times & \xrightarrow{\psi_{L'/K}} & \mathrm{Gal}(L'/K)^{\mathrm{ab}} \\ \| & & \downarrow \pi \\ K^\times & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \end{array}$$

Here π is induced by the canonical projection $\mathrm{Gal}(L'/K) \to \mathrm{Gal}(L/K)$.

Proof. Write G and G' for $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L'/K)$ respectively. Let $a \in K^\times$. Let $g = \psi_{L/K}(a) \in G^{\mathrm{ab}}$, and let $g' = \psi_{L'/K}(a) \in G'^{\mathrm{ab}}$. We need to show that $\pi(g') = g$.

Let $f \in \widehat{\mathbf{H}}^1(G, \mathbb{Q}/\mathbb{Z})$ be an arbitrary element, and let $f' = \mathrm{Inf}(f) \in \widehat{\mathbf{H}}^1(G', \mathbb{Q}/\mathbb{Z})$. If we think of f and f' as characters $G^{\mathrm{ab}} \to \mathbb{Q}/\mathbb{Z}$ and $G'^{\mathrm{ab}} \to \mathbb{Q}/\mathbb{Z}$, then $f' = f \circ \pi$. By duality, in order to show that $\pi(g') = g$, we only need to show that $f'(g') = f(g)$.

By Lemma 1.24.3 we have

$$f'(g') = \mathrm{inv}(\bar{a} \cup \delta f')$$

Since the operations $\delta(\cdot), \bar{a} \cup \cdot$, and $\mathrm{inv}(\cdot)$ are all compatible with inflation, the right hand side is equal to $\mathrm{inv}(\bar{a} \cup \delta f)$, which is equal to $f(g)$. □

By Lemma 1.24.6, we can define the local Artin map

$$\psi_K : K^\times \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

by taking the inverse limit of $\psi_{L/K}$ over all finite abelian extensions L/K. Comparing with the statement of Theorem 1.1.1, we see that condition (ii) in that theorem is satisfied by construction. We still need to check condition (i):

Lemma 1.24.7. *Let $\pi \in K$ be a uniformizer. Then $\psi_K(\pi)$ acts as the Frobenius σ on K^{ur}.*

Proof. Let n be an arbitrary positive integer. Write G for $\mathrm{Gal}(K_n/K)$, where K_n/K is the degree n unramified extension. Let $\sigma' = \psi_{K_n/K}(\pi)$. It suffices to show that σ' is equal to the Frobenius $\sigma \in G$. Let $f \in \widehat{\mathbf{H}}^1(G, \mathbb{Q}/\mathbb{Z})$. We have

$$f(\sigma') = \mathrm{inv}(\bar{\pi} \cup \delta f).$$

Recall that $\mathrm{inv} : \mathrm{Br}(K_n/K) \xrightarrow{\sim} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ is the composition

$$\mathrm{Br}(K_n/K) \xrightarrow{v} \widehat{\mathbf{H}}^2(G, \mathbb{Z}) \xrightarrow{\delta^{-1}} \widehat{\mathbf{H}}^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{ev}_\sigma} \mathbb{Q}/\mathbb{Z},$$

where ev_σ is the evaluation of elements of $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ at σ. We have $v(\bar{\pi} \cup \delta f) = v(\pi) \cdot \delta f = \delta f$. Hence

$$f(\sigma') = \mathrm{ev}_\sigma \circ \delta^{-1}(\delta(f)) = \mathrm{ev}_\sigma(f) = f(\sigma).$$

Since f is arbitrary, this shows that $\sigma = \sigma'$. □

We have finished the proof of Theorem 1.1.1.

Exercise 1.24.8. Show that $\mathrm{Br}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. Let u be a generator. Show that $u \cup \cdot$ defines an isomorphism $\widehat{\mathbf{H}}^q(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{Z}) \xrightarrow{\sim} \widehat{\mathbf{H}}^{q+2}(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times)$ for all q. Compute these groups for all q.

1.25. **Functorial properties of the local Artin map.** As a bonus of the cohomological method, we can easily prove the norm and transfer functoriality of the local Artin map.

Proof of Theorem 1.1.3. Let L be a common finite Galois extension of K' and K. Let $G = G_{L/K}$ and $H = G_{L/K'} \leq G$. It suffices to prove the commutativity of the following diagrams:

$$\begin{array}{ccc} \widehat{\mathbf{H}}^0(H, L^\times) & \xleftarrow{u_{L/K'} \cup \cdot} & \widehat{\mathbf{H}}^{-2}(H, \mathbb{Z}) \\ \Big\downarrow{\scriptstyle \mathrm{Cor}} & & \Big\downarrow{\scriptstyle \mathrm{Cor}} \\ \widehat{\mathbf{H}}^0(G, L^\times) & \xleftarrow{u_{L/K} \cup \cdot} & \widehat{\mathbf{H}}^{-2}(G, \mathbb{Z}) \end{array} \qquad \begin{array}{ccc} \widehat{\mathbf{H}}^0(H, L^\times) & \xleftarrow{u_{L/K'} \cup \cdot} & \widehat{\mathbf{H}}^{-2}(H, \mathbb{Z}) \\ \Big\uparrow{\scriptstyle \mathrm{Res}} & & \Big\uparrow{\scriptstyle \mathrm{Res}} \\ \widehat{\mathbf{H}}^0(G, L^\times) & \xleftarrow{u_{L/K} \cup \cdot} & \widehat{\mathbf{H}}^{-2}(G, \mathbb{Z}) \end{array}$$

For the second diagram, we use $\mathrm{Res}(u_{L/K}) = u_{L/K'}$, which follows from Lemma 1.22.1, and we use the formula $\mathrm{Res}(a \cup b) = \mathrm{Res}(a) \cup \mathrm{Res}(b)$. For the first diagram, we must show $u_{L/K} \cup \mathrm{Cor}(\beta) = \mathrm{Cor}(u_{L/K'} \cup \beta)$. Now the right hand side is

$$\mathrm{Cor}(\mathrm{Res}(u_{L/K}) \cup \beta) = u_{L/K} \cup \mathrm{Cor}(\beta).$$

□

2. Global class field theory via cohomology

2.1. **Statements of global class field theory.** We start by briefly reviewing adeles and ideles. Let K be a global field. Let V_K denote the set of places of K, and $V_{K,\infty}$ (resp. $V_{K,f}$) the set of archimedean (resp. non-archimedean) places. The ring of adeles for K is the restricted product

$$\mathbb{A}_K := \prod_{v\in V_K}{}' K_v$$

with respect to $\mathcal{O}_{K_v}$ for $v \in V_{K,f}$. Its group of units is the group of ideles, which is the restricted product

$$\mathbb{A}_K^\times := \prod_{v\in V_K}{}' K_v^\times$$

with respect to $\mathcal{O}_{K_v}^\times$ for $v \in V_{K,f}$. Both $\mathbb{A}_K$ and $\mathbb{A}_K^\times$ are equipped with the restricted product topology. For every finite subset $S \subset V_K$ such that $S \supset V_{K,\infty}$, consider the ring

$$\mathbb{A}_{K,S} = \prod_{v\in S} K_v \times \prod_{v\in V_K - S} \mathcal{O}_{K_v}.$$

Its group of units is

$$\mathbb{A}_{K,S}^\times = \prod_{v\in S} K_v^\times \times \prod_{v\in V_K - S} \mathcal{O}_{K_v}^\times.$$

We have

$$\mathbb{A}_K = \bigcup_S \mathbb{A}_{K,S}, \quad \mathbb{A}_K^\times = \bigcup_S \mathbb{A}_{K,S}^\times.$$

Each $\mathbb{A}_{K,S}$ (resp. $\mathbb{A}_{K,S}^\times$) is open in $\mathbb{A}_K$ (resp. $\mathbb{A}_K^\times$), and the subspace topology on $\mathbb{A}_{K,S}$ (resp. $\mathbb{A}_{K,S}^\times$) inherited from $\mathbb{A}_K$ (resp. $\mathbb{A}_K^\times$) agrees with the product topology.

We have diagonal embeddings $K \hookrightarrow \mathbb{A}_K$ and $K^\times \hookrightarrow \mathbb{A}_K^\times$. Define the idele class group

$$C_K := \mathbb{A}_K^\times / K^\times.$$

Let L/K be a finite extension. Then there is a natural injective homomorphism $i : \mathbb{A}_K \hookrightarrow \mathbb{A}_L$ whose restriction to the diagonally embedded K is just the inclusion $K \hookrightarrow L$. The injection i extends to an L-algebra isomorphism $L \otimes_K \mathbb{A}_K \xrightarrow{\sim} \mathbb{A}_L$. Moreover, i restricts to an injective homomorphism $\mathbb{A}_K^\times \to \mathbb{A}_L^\times$, which further induces an injective homomorphism $C_K \to C_L$. Furthermore, we have a norm map $\mathrm{N}_{L/K} : \mathbb{A}_L^\times \to \mathbb{A}_K^\times$ whose restriction to the diagonally embedded $L^\times$ is the usual norm $L^\times \to K^\times$. This induces a norm map $\mathrm{N}_{L/K} : C_L \to C_K$.

Theorem 2.1.1 (Reciprocity Law)**.** *There is a continuous homomorphism $\psi_K : C_K \to G_K^{\mathrm{ab}}$ satisfying the following properties for all finite abelian extensions L/K. We write $\psi_{L/K}$ for the composite map $C_K \xrightarrow{\psi_K} G_K^{\mathrm{ab}} \to \mathrm{Gal}(L/K)$.*

1. *For each $v \in V_K$, consider the composite map $f_v : K_v^\times \to C_K \xrightarrow{\psi_{L/K}} \mathrm{Gal}(L/K)$. If v is non-archimedean, then f_v kills $\mathcal{O}_{K_v}^\times$ if and only v is unramified in L. When this holds, f_v sends any uniformizer to $\mathrm{Frob}_v \in \mathrm{Gal}(L/K)$. If v is archimedean and unramified in L (i.e., either v is complex or every place of L above v is real), then $f_v = 1$. If v is archimedean and ramifies in L (i.e., v is real and every place of L above v is complex) then f_v factors through the sign map $K_v^\times = \mathbb{R}^\times \to \{\pm 1\}$ and*

sends -1 *to the complex conjugation in* $\mathrm{Gal}(L/K)$ *arising from a complex embedding* $L \hookrightarrow \mathbb{C}$ *corresponding to a complex place above* v.

(2) *The map* $\psi_{L/K}$ *is surjective, and its kernel is* $\mathrm{N}_{L/K}(C_L)$.

Remark 2.1.2. Last semester, we already saw that condition (1) for almost all places $v \in V_K$ already uniquely characterizes $\psi_{L/K}$. Hence ψ_K is unique.

Theorem 2.1.3 (Existence Theorem)**.** *A subgroup of* C_K *is open and of finite index if and only if it is of the form* $\mathrm{N}_{L/K}(C_L)$ *for a finite abelian extension* L/K.

Remark 2.1.4. Theorem 2.1.1 implies the "if" direction in Theorem 2.1.3.

Theorems 2.1.1 and 2.1.3 are the two main theorems of global class field theory. In addition to these, we have norm and transfer functoriality, and local-global compatibility.

Theorem 2.1.5 (Norm and transfer functoriality)**.** *Let* L/K *be a finite separable extension. Then we have a commutative diagram*

$$\begin{array}{ccc} C_L & \xrightarrow{\psi_L} & G_L^{\mathrm{ab}} \\ {\scriptstyle \mathrm{N}_{L/K}}\downarrow & & \downarrow{\scriptstyle i} \\ C_K & \xrightarrow{\psi_K} & G_K^{\mathrm{ab}} \end{array}$$

where i *is induced by the inclusion* $G_L \hookrightarrow G_K$. *We have a commutative diagram*

$$\begin{array}{ccc} C_L & \xrightarrow{\psi_L} & G_L^{\mathrm{ab}} \\ \uparrow & & \uparrow{\scriptstyle V} \\ C_K & \xrightarrow{\psi_K} & G_K^{\mathrm{ab}} \end{array}$$

where V *is the transfer map.*

To state local-global compatibility, let v be a (finite) place of K and choose a K-algebra embedding $i : K^s \hookrightarrow (K_v)^s$. This determines a place of K^s above v, as well as a closed embedding $G_{K_v} \hookrightarrow G_K$ whose image is the decomposition group of that place. The induced map $G_{K_v}^{\mathrm{ab}} \to G_K^{\mathrm{ab}}$ is independent of the choice of i.

Theorem 2.1.6 (Local-global compatibility)**.** *We have a commutative diagram*

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\psi_{K_v}} & G_{K_v}^{\mathrm{ab}} \\ \downarrow & & \downarrow \\ C_K & \xrightarrow{\psi_K} & G_K^{\mathrm{ab}}. \end{array}$$

The idea of proof of Theorem 2.1.1 is again to apply Tate's theorem to $\widehat{\mathbf{H}}^2(\mathrm{Gal}(L/K), C_L)$ for a finite Galois extension L/K. We shall prove:

- $\widehat{\mathbf{H}}^1(\mathrm{Gal}(L/K), C_L) = 0$.
- $\widehat{\mathbf{H}}^2(\mathrm{Gal}(L/K), C_L) \cong \mathbb{Z}/[L:K]\mathbb{Z}$.

Thus by Tate's theorem, there is a fundamental class $u_{L/K} \in \widehat{\mathbf{H}}^2(\mathrm{Gal}(L/K), C_L)$ such that for all $q \in \mathbb{Z}$ the map $u_{L/K} \cup \cdot : \widehat{\mathbf{H}}^q(\mathrm{Gal}(L/K), \mathbb{Z}) \to \widehat{\mathbf{H}}^{q+2}(\mathrm{Gal}(L/K), C_L)$ is an

isomorphism. It also turns out that $(C_L)^{\mathrm{Gal}(L/K)} = C_K$. Thus for $q = -2$ we obtain an isomorphism

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} \xrightarrow{\sim} C_K/\mathrm{N}_{L/K}(C_L).$$

We then define $\psi_{L/K}$ to be the inverse.

2.2. **Cohomology of ideles.** Let L/K be a finite Galois extension of global fields, and write G for $\mathrm{Gal}(L/K)$. We study $\widehat{\mathbf{H}}^q(G, \mathbb{A}_L^\times)$.

Consider finite subsets $S \subset V_K$ containing $V_{K,\infty}$ and all the finite places of V_K which ramify in L. Write $\mathbb{A}_{L,S}^\times$ for

$$\prod_{v\in S}\prod_{w\in V_L, w|v} L_w^\times \times \prod_{v\in V_K - S}\prod_{w\in V_L, w|v} \mathcal{O}_{L_w}^\times.$$

In other words, if T is the set of places of L above S, then $\mathbb{A}_{L,S}^\times := \mathbb{A}_{L,T}^\times$. Note that $\mathbb{A}_{L,S}^\times$ is a G-submodule of $\mathbb{A}_L^\times$, and we have $\mathbb{A}_L^\times = \varinjlim_S \mathbb{A}_{L,S}^\times$.

Recall that for any G-module X, $\widehat{\mathbf{H}}^q(G, X)$ is the q-th cohomology of $\mathrm{Hom}_{\mathbb{Z}[G]}(P_\bullet, X)$, where $(P_\bullet)_{\bullet\in\mathbb{Z}}$ is a complete resolution of $\mathbb{Z}$. Since each P_i is a finite rank free $\mathbb{Z}[G]$-module, the functor $\mathrm{Hom}_{\mathbb{Z}[G]}(P_i, \cdot)$ commutes with direct limits. Also taking the q-th cohomology of a complex commutes with direct limits of complexes. Hence $\widehat{\mathbf{H}}^q(G, \cdot)$ commutes with direct limits. In particular,

$$\widehat{\mathbf{H}}^q(G, \mathbb{A}_L^\times) \cong \varinjlim_S \widehat{\mathbf{H}}^q(G, \mathbb{A}_{L,S}^\times).$$

Exercise 2.2.1. Let G be a finite group, and let I be a set with a transitive G-action. Suppose X is a G-module and it can be written as $\bigoplus_{i\in I} X_i$ such that for each $i \in I$ and $g \in G$, the action of g on X induces an isomorphism $X_i \to X_{g(i)}$. Then, for any $i_0 \in I$, we have an isomorphism of G-modules $X \cong \mathrm{Ind}_{G_{i_0}}^G X_{i_0}$. Here G_{i_0} denotes the stabilizer of i_0 in G and it acts on X_{i_0}.

By the exercise, we have

$$\mathbb{A}_{L,S}^\times \cong \prod_{v\in S} \mathrm{Ind}_{D(w/v)}^G L_w^\times \times \prod_{v\in V_K - S} \mathrm{Ind}_{D(w/v)}^G \mathcal{O}_{L_w}^\times$$

where for each v we choose a place $w|v$ and denote by $D(w/v)$ the decomposition group as usual. By Shapiro's Lemma for Tate cohomology (Proposition 1.14.3), we obtain

$$\widehat{\mathbf{H}}^q(G, \mathbb{A}_{L,S}^\times) \cong \prod_{v\in S} \widehat{\mathbf{H}}^q(\mathrm{Gal}(L_w/K_v), L_w^\times) \times \prod_{v\in V_K - S} \widehat{\mathbf{H}}^q(\mathrm{Gal}(L_w/K_v), \mathcal{O}_{L_w}^\times).$$

For $v \in V_K - S$, the extension L_w/K_v is unramified, and so $\widehat{\mathbf{H}}^q(\mathrm{Gal}(L_w/K_v), \mathcal{O}_{L_w}^\times) = 0$ (see Proposition 1.21.1). We obtain the following conclusion:

Proposition 2.2.2. *We have*

$$\widehat{\mathbf{H}}^q(G, \mathbb{A}_{L,S}^\times) \cong \prod_{v\in S} \widehat{\mathbf{H}}^q(\mathrm{Gal}(L_w/K_v), L_w^\times)$$

and

$$\widehat{\mathbf{H}}^q(G, \mathbb{A}_L^\times) \cong \varinjlim_S \widehat{\mathbf{H}}^q(G, \mathbb{A}_{L,S}^\times) \cong \bigoplus_{v\in V_K} \widehat{\mathbf{H}}^q(\mathrm{Gal}(L_w/K_v), L_w^\times).$$

□

Corollary 2.2.3. *We have* $\widehat{\mathbf{H}}^1(G, \mathbb{A}_L^\times) = 0$, *and* $\widehat{\mathbf{H}}^2(G, \mathbb{A}_L^\times) \cong \bigoplus_{v \in V_K} \mathrm{Br}(L_w/K_v) \cong \bigoplus_{v \in V_K} \mathbb{Z}/[L_w : K_v]$. *For each* $q \in \mathbb{Z}$, *we have*

$$\widehat{\mathbf{H}}^q(G, \mathbb{A}_L^\times) \cong \bigoplus_{v \in V_K} \widehat{\mathbf{H}}^{q-2}(\mathrm{Gal}(L_w/K_v), \mathbb{Z}).$$

Example 2.2.4. We have $\widehat{\mathbf{H}}^3(G, \mathbb{A}_L^\times) = 0$ since $\widehat{\mathbf{H}}^1(\mathrm{Gal}(L_w/K_v), \mathbb{Z}) = \mathrm{Hom}(\mathrm{Gal}(L_w/K_v), \mathbb{Z}) = 0$.

By a similar argument, we have

$$(\mathbb{A}_L^\times)^G = \varinjlim_S \prod_{v \in S} (L_w^\times)^{\mathrm{Gal}(L_w/K_v)} \times \prod_{v \in V_K - S} (\mathcal{O}_{L_w}^\times)^{\mathrm{Gal}(L_w/K_v)} = \varinjlim_S \mathbb{A}_{K,S}^\times = \mathbb{A}_K.$$

Proposition 2.2.5. *We have* $(C_L)^G = C_K$.

Proof. We have an exact sequence $0 \to (L^\times)^G \to (\mathbb{A}_L^\times)^G \to (C_L)^G \to \mathbf{H}^1(G, L^\times)$. The last term is zero by Hilbert 90. □

2.3. **Herbrand quotient for the idele class group (the First Inequality).** For a finite Galois extension L/K, one of our ultimate goals is to establish an isomorphism $C_K/\mathrm{N}_{L/K} C_L \xrightarrow{\sim} \mathrm{Gal}(L/K)$, so we expect

$$[C_K : \mathrm{N}_{L/K} C_L] = [L : K].$$

Also, in order to apply Tate's theorem we need to show that $\widehat{\mathbf{H}}^2(\mathrm{Gal}(L/K), C_L) \cong \mathbb{Z}/[L : K]$ and $\widehat{\mathbf{H}}^1(\mathrm{Gal}(L/K), C_L) = 0$. Hence in the case of a cyclic extension L/K we expect that the Herbrand quotient of the $\mathrm{Gal}(L/K)$-module C_L is

$$h(C_L) = [L : K].$$

Theorem 2.3.1. *Let* L/K *be a finite cyclic extension. Then the Herbrand quotient of the* $\mathrm{Gal}(L/K)$*-module* C_L *is defined, and it is equal to* $[L : K]$.

Corollary 2.3.2 (The First Inequality)**.** *For a finite cyclic extension* L/K, *we have*

$$[C_K : \mathrm{N}_{L/K} C_L] \geq [L : K].$$

Proof. The left hand side is $h^0(C_L)$ (by Proposition 2.2.5), and the right hand side is $h(C_L) = h^0(C_L)/h^1(C_L)$. □

In order to prove Theorem 2.3.1 we need the following lemma.

Lemma 2.3.3. *Let* M_1, M_2 *be two* G*-modules. Assume that for some field* $F \supset \mathbb{Q}$ *there exists an* $F[G]$*-module isomorphism* $M_1 \otimes_{\mathbb{Z}} F \xrightarrow{\sim} M_2 \otimes_{\mathbb{Z}} F$. *Then there exists a* $\mathbb{Q}[G]$*-module isomorphism* $M_1 \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\sim} M_2 \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proof. For any field $F \supset \mathbb{Q}$, let H_F be the set of all F-linear maps $M_1 \otimes F \to M_2 \otimes F$, and let $H_F^G \subset H_F$ be the subset of $F[G]$-linear maps. Clearly $H_F \cong H_{\mathbb{Q}} \otimes_{\mathbb{Q}} F$, and $H_F^G \subset H_F$ is defined by a system of $\mathbb{Q}$-coefficient homogeneous linear equations which are independent of F. In other words, $H_{\mathbb{Q}}^G$ is a $\mathbb{Q}$-subspace of $H_{\mathbb{Q}}$ and we have $H_F^G \cong H_{\mathbb{Q}}^G \otimes_{\mathbb{Q}} F$. By our assumption, there exists a field $F \supset \mathbb{Q}$, elements $t_1, \ldots, t_d \in F$ and $\phi_1, \ldots, \phi_d \in H_{\mathbb{Q}}^G$ such that $t_1\phi_1 + \cdots + t_d\phi_d$ is an isomorphism. In particular M_1 and M_2 have the same rank, and if we fix a basis of each and view all elements of H_F as square matrices, we have

$$\det(t_1\phi_1 + \cdots + t_d\phi_d) \neq 0.$$

Since the above is a $\mathbb{Q}$-coefficient polynomial in the variables $t_1, \dots, t_d$, there exists $s_1, \dots, s_d \in \mathbb{Q}$ such that

$$\det(s_1\phi_1 + \cdots + s_d\phi_d) \neq 0.$$

Then $s_1\phi_1 + \cdots + s_d\phi_d$ is an element of $H^G_{\mathbb{Q}}$ which is an isomorphism. □

We also need to recall some facts established in the last semester.

Fact 2.3.4. *Let T be a non-empty finite subset of V_L containing $V_{L,\infty}$. Then $\mathbb{A}_L^\times/(L^\times \mathbb{A}_{L,T}^\times)$ is finite.*

Let $\mathcal{O}_{L,T} = L \cap \mathbb{A}_{L,T}$. Its group of units is $\mathcal{O}_{L,T}^\times = L^\times \cap \mathbb{A}_{L,T}^\times$. The group $\mathbb{A}_L^\times/(L^\times \mathbb{A}_{L,T}^\times)$ is identified with the class group of $\mathcal{O}_{L,T}$, and we proved the finiteness last semester based on the compactness of $(\mathbb{A}_L^\times)^1/L^\times$.

As a consequence, since $\mathbb{A}_L^\times = \bigcup_T \mathbb{A}_{L,T}^\times$, we can take T large enough so that $\mathbb{A}_{L,T}^\times$ contains a set of representatives of the finitely many elements of $\mathbb{A}_L^\times/(L^\times \mathbb{A}_{L,T_0}^\times)$ for some fixed T_0. For such T we then have $\mathbb{A}_L^\times = L^\times \mathbb{A}_{L,T}^\times$.

Last semester we also proved Dirichlet's unit theorem for $\mathcal{O}_{L,T}^\times$, which states that it is a finitely generated abelian group with rank $|T| - 1$. During the proof we established the following result:

Fact 2.3.5. *Let $l : \mathcal{O}_{L,T}^\times \to \mathbb{R}^T, x \mapsto (\log \|x\|_w)_{w\in T}$. Then l has finite kernel, and its image is a full rank lattice in the hyperplane $H := \{(r_w) \in \mathbb{R}^T \mid \sum_{w\in T} r_w = 0\}$.*

Proof of Theorem 2.3.1. Write G for $\mathrm{Gal}(L/K)$. Take a finite subset $S \subset V_K$ containing $V_{K,\infty}$ and all finite places which ramify in L, and large enough such that the set T of places of L above S satisfy $\mathbb{A}_L^\times = L^\times \mathbb{A}_{L,T}^\times$. We then have a short exact sequence of G-modules

$$1 \to \mathcal{O}_{L,T}^\times \to \mathbb{A}_{L,T}^\times \to C_L \to 1.$$

It suffices to show that the Herbrand quotients of $\mathcal{O}_{L,T}^\times$ and $\mathbb{A}_{L,T}^\times$ are defined and compute them.

For $\mathbb{A}_{L,T}^\times$, by Proposition 2.2.2 we have

$$\widehat{\mathbf{H}}^q(G, \mathbb{A}_{L,T}^\times) \cong \prod_{v\in S} \widehat{\mathbf{H}}^q(\mathrm{Gal}(L_w/K_v), L_w^\times).$$

Hence the Herbrand quotient of $\mathbb{A}_{L,T}^\times$ is defined and is equal to the product of local Herbrand quotients (note that each $\mathrm{Gal}(L_w/K_v)$ is a subgroup of $\mathrm{Gal}(L/K)$ and hence cyclic):

$$h(\mathbb{A}_{L,T}^\times) = \prod_{v\in S} \frac{\#\widehat{\mathbf{H}}^2(\mathrm{Gal}(L_w/K_v), L_w^\times)}{\#\widehat{\mathbf{H}}^1(\mathrm{Gal}(L_w/K_v), L_w^\times)} = \prod_{v\in S} [L_w : K_v].$$

Now consider $\mathcal{O}_{L,T}^\times$. Let G act on $\mathbb{R}^T$ by its permutation of T. Since $l : \mathcal{O}_{L,T}^\times \to \mathbb{R}^T$ has finite kernel and is clearly a G-map, the Herbrand quotient of $\mathcal{O}_{L,T}^\times$ is defined if and only if the Herbrand quotient of $\Lambda := l(\mathcal{O}_{L,T}^\times)$ is defined, and when this is the case they are equal. Let $e = (1, \dots, 1) \in \mathbb{R}^T$, which is fixed by $\mathrm{Gal}(L/K)$. Let $M_1 = \Lambda \oplus \mathbb{Z}e \subset \mathbb{R}^T$. We know $h(\mathbb{Z}) = [L : K]$ (see Example 1.17.5), so it remains to show that the Herbrand quotient of M_1 is defined and compute it. Then we would get $h(\mathcal{O}_{L,T}^\times) = h(\Lambda) = h(M_1)/[L : K]$

Let $M_2 = \mathbb{Z}^T \subset \mathbb{R}^T$. It is a G-submodule, and isomorphic to $\prod_{v\in S} \mathrm{Ind}_{\mathrm{Gal}(L_w/K_v)}^G \mathbb{Z}$ by Exercise 2.2.1. Therefore

$$h(M_2) = \prod_{v\in S} \frac{\#\widehat{\mathbf{H}}^0(\mathrm{Gal}(L_w/K_v),\mathbb{Z})}{\#\widehat{\mathbf{H}}^{\pm 1}(\mathrm{Gal}(L_w/K_v),\mathbb{Z})} = \prod_{v\in S}[L_w : K_v].$$

Finally, since M_1 and M_2 are two full rank G-stable lattices in $\mathbb{R}^T$, applying Lemma 2.3.3 we get an injective G-map $M_1 \to M_2$ with finite cokernel. Hence $h(M_1) = h(M_2)$. Combining the results we have

$$h(\mathcal{O}_{L,T}^\times) = h(\Lambda) = h(M_1)/[L:K] = h(M_2)/[L:K] = [L:K]^{-1}\prod_{v\in S}[L_w : K_v],$$

$$h(C_L) = h(\mathbb{A}_{L,T}^\times)/h(\mathcal{O}_{L,T}^\times) = \frac{\prod_{v\in S}[L_w:K_v]}{[L:K]^{-1}\prod_{v\in S}[L_w:K_v]} = [L:K].$$

□

Corollary 2.3.6. *Let L/K be a non-trivial finite Galois extension with solvable Galois group. The following statements hold.*

(1) *There are infinitely many places of K which do not split in L.*
(2) *For any finite subset $T \subset V_L$, $\mathrm{Gal}(L/K)$ is generated by $\{\mathrm{Frob}(w/K) \mid w \in V_L - T, w$ is unramified over $K\}$.*

Proof. For (1), there is a non-trivial cyclic extension L'/K inside L and it suffices to show that there are infinitely many places of K which do not split in L'. Hence we may assume that L/K is cyclic. Suppose there are only finitely many places of K which do not split in L. Let S be the set of these places. Let $B = \{(x_v) \in \mathbb{A}_K^\times \mid x_v = 1, \forall v \in S\}$. Then clearly $B \subset \mathrm{N}_{L/K}\mathbb{A}_L^\times$. Last semester we showed that the image of B in C_K is dense. Hence $\mathrm{N}_{L/K}C_L$ is dense in C_K. On the other hand, $\mathrm{N}_{L/K}(\mathbb{A}_L^\times)$ is open in $\mathbb{A}_K^\times$ since $\mathrm{N}_{L_w/K_v}L_w^\times$ is open in $K_v^\times$ for every $w|v$ by local class field theory and $\mathrm{N}_{L_w/K_v}\mathcal{O}_{L_w}^\times = \mathcal{O}_{K_v}^\times$ for every unramified $w|v$ (see Remark 1.21.4). Therefore $\mathrm{N}_{L/K}C_L$ is an open, and hence closed, subgroup of C_K. Thus $C_K = \mathrm{N}_{L/K}C_L$. This contradicts with the First Inequality $[C_K : \mathrm{N}_{L/K}C_L] \geq [L:K]$.

For (2), let G' be the subgroup of $\mathrm{Gal}(L/K)$ generated by the set in question. Let $K' = L^{G'}$. Then every $v \in V_K$ which is unramified in L and which does not lie below T is split in K', since for every $u \in V_{K'}$ above v we have $\mathrm{Frob}(u/v) = 1$. There are infinitely many such v, so by part (1) we know that $K' = K$. It follows that $G' = G$. □

Remark 2.3.7. In the proof we saw that (2) is a formal consequence of (1). Statement (1) itself is a weak consequence of the Chebotarev density theorem, which asserts that the set of places of K which do not split in L has Dirichlet density $1 - [L:K]^{-1}$.

2.4. **Upper bound for the cohomology of the idele class group (the Second Inequality).** Let L/K be a finite Galois extension of global fields, and write G for $\mathrm{Gal}(L/K)$. Recall that we expect that $\widehat{\mathbf{H}}^2(G,C_L) \cong \mathbb{Z}/[L:K]\mathbb{Z}$ and $\widehat{\mathbf{H}}^1(G,C_L) = 0$. Also we expect to have an isomorphism $G^{\mathrm{ab}} \xrightarrow{\sim} \widehat{\mathbf{H}}^0(G,C_L)$ by cupping with the fundamental class, so at least $|\widehat{\mathbf{H}}^0(G,C_L)|$ should divide $[L:K]$.

Our current goal is to prove the following upper bounds.

Theorem 2.4.1. *The following statements hold:*

(1) $\widehat{\mathbf{H}}^1(G,C_L) = 0$.
(2) $|\widehat{\mathbf{H}}^0(G,C_L)|$ *divides* $[L:K]$.

(3) $|\widehat{\mathbf{H}}^2(G, C_L)|$ *divides* $[L : K]$.

We first reduce the theorem to the case of a cyclic extension L/K of prime degree. The argument is essentially the same as in the proof of Theorem 1.22.4. For each prime p dividing $[L : K]$ and a Sylow p-subgroup G_p of G, since the composition $\widehat{\mathbf{H}}^i(G, C_L) \xrightarrow{\text{Res}} \widehat{\mathbf{H}}^i(G_p, C_L) \xrightarrow{\text{Cor}} \widehat{\mathbf{H}}^i(G, C_L)$ is $[G : G_p]$, the map $\text{Res} : \widehat{\mathbf{H}}^i(G, C_L) \to \widehat{\mathbf{H}}^i(G_p, C_L)$ is injective on the p-primary part. Hence we have reduced all three statements to the case of a solvable extension. Then part (1) reduces to the prime degree case by the inflation-restriction exact sequence for $\widehat{\mathbf{H}}^1$. Once we have established the triviality of $\widehat{\mathbf{H}}^1(G, C_L)$, we also know this for all subgroups of G, and as a result we have inflation-restriction exact sequence for $\widehat{\mathbf{H}}^2$. Then (3) in the solvable case reduces to the prime degree case by induction. For (2), if N is a normal subgroup of G and $L' = L^N$, then we have an exact sequence

$$C_{L'}/\mathrm{N}_{L/L'}C_L \xrightarrow{\mathrm{N}_{L'/K}} C_K/\mathrm{N}_{L/K}C_L \to C_K/\mathrm{N}_{L'/K}C_{L'} \to 1$$

Hence (2) in the solvable case follows from the prime degree case and induction.

Once we are in the cyclic case, the three statements in the theorem are actually all equivalent to the inequality

$$|\widehat{\mathbf{H}}^0(G, C_L)| = [C_K : \mathrm{N}_{L/K}C_L] \le [L : K],$$

which is called *the Second Inequality*. This is because we have periodicity 2 for the cohomology and we already know that the Herbrand quotient $h(C_L) = [L : K]$.

Thus we have reduced Theorem 2.4.1 to the following theorem:

Theorem 2.4.2. *Let L/K be a cyclic extension of prime degree p. Then we have the Second Inequality:*

$$[C_K : \mathrm{N}_{L/K}C_L] \le [L : K].$$

We first prove the theorem assuming that p is not the characteristic of K (e.g., K is a number field). Let μ_p denote the group of all p-th roots of unity in K^s.

Lemma 2.4.3. *In order to prove Theorem 2.4.2 when* $\mathrm{char} K \neq p$*, we may assume that K contains μ_p.*

Proof. Assume that K does not contain μ_p. Let $K' = K(\mu_p)$ and $L' = L(\mu_p)$. Since $[K' : K]$ divides $p - 1$ and is coprime to p, K' and L are linearly disjoint over K. It follows that we have a commutative diagram

$$\begin{array}{ccc} C_L & \xrightarrow{\mathrm{N}_{L/K}} & C_K \\ {\scriptstyle i_L}\downarrow & & \downarrow{\scriptstyle i_K} \\ C_{L'} & \xrightarrow{\mathrm{N}_{L'/K'}} & C_{K'} \\ {\scriptstyle \mathrm{N}_{L'/L}}\downarrow & & \downarrow{\scriptstyle \mathrm{N}_{K'/K}} \\ C_L & \xrightarrow{\mathrm{N}_{L/K}} & C_K \end{array}$$

where i_L and i_K are induced by the inclusions $L \hookrightarrow L'$ and $K \hookrightarrow K'$ respectively. In particular, the two arrows in the second column induce homomorphisms $\phi : C_K/\mathrm{N}_{L/K}C_L \to C_{K'}/\mathrm{N}_{L'/K'}C_{L'}$ and $\psi : C_{K'}/\mathrm{N}_{L'/K'}C_{L'} \to C_K/\mathrm{N}_{L/K}C_L$. But $\psi \circ \phi$ is multiplication by $[K' : K]$, and this is an automorphism since $C_K/\mathrm{N}_{L/K}C_L = \widehat{\mathbf{H}}^0(\mathrm{Gal}(L/K), C_L)$ is p-torsion. Hence ϕ is injective. The desired inequality for the extension L/K thus follows from that for L'/K', which is also a cyclic extension of degree p. □

When $K \supset \mu_p$, degree p cyclic extensions of K are controlled by *Kummer theory*. Let us recall it. Let K be a field, and n be a positive integer not divisible by $\mathrm{char}K$. Assume that K contains the full group μ_n of n-th roots of unity. We call an algebraic extension L/K a *Kummer extension with respect to* n, if it is abelian and $\mathrm{Gal}(L/K)$ is killed by n.

Fact 2.4.4 (Kummer theory)**.** *An algebraic extension L/K is a Kummer extension with respect to n if and only if L is of the form $K(\{\sqrt[n]{a} \mid a \in A\})$ for a subset A of $K^\times$. We have a bijection*

$$\{\textit{Kummer extensions of } K \textit{ in } K^s \textit{ with respect to } n\} \xrightarrow{\sim} \{\textit{subgroups of } K^\times/(K^\times)^n\}$$

sending L/K to $(K^\times \cap (L^\times)^n))/K^\times$, and the inverse map sends A to $L = K(\{\sqrt[n]{a} \mid a \in A\})$. Assume that L/K corresponds to A under the bijection. Then we have a bi-multiplicative pairing

$$\begin{aligned} \mathrm{Gal}(L/K) \times A &\longrightarrow \mu_n \\ (g, a) &\longmapsto \frac{g\sqrt[n]{a}}{\sqrt[n]{a}}. \end{aligned}$$

Here, for each $a \in A$, we choose an n-th root $\sqrt[n]{a} \in L^\times$ of (a representative in $K^\times$ of) a, and the pairing is independent of this choice since a different choice differs by an element of μ_n which is fixed by $\mathrm{Gal}(L/K)$. This pairing induces an isomorphism of topological groups

$$\mathrm{Gal}(L/K) \xrightarrow{\sim} A^\vee := \mathrm{Hom}(A, \mu_n),$$

where the topology on $\mathrm{Hom}(A, \mu_n)$ is the profinite topology induced by the identification $\mathrm{Hom}(A, \mu_n) = \varprojlim_{\textit{finite subgroups } A' \leq A} \mathrm{Hom}(A', \mu_n)$, and an isomorphism of abstract groups

$$A \xrightarrow{\sim} \mathrm{Gal}(L/K)^\vee := \mathrm{Hom}_{cont}(\mathrm{Gal}(L/K), \mu_n).$$

In particular, $[L : K]$ is finite if and only if A is finite, and in this case we have $[L : K] = |A|$.

Remark 2.4.5. Since $\mathrm{Gal}(L/K)$ and A are abelian groups killed by n, $\mathrm{Gal}(L/K)^\vee$ and $A^\vee$ here are just the usual Pontryagin duals of the respective groups, namely the groups of continuous homomorphisms to S^1. (Here $\mathrm{Gal}(L/K)$ has the usual Krull topology and A has discrete topology.) In general, for any locally compact Hausdorff abelian group, its Pontryagin dual equipped with the "compact-open topology" is also a topological group of the same type, and the double dual is canonically isomorphic to the original group. It is a fact that the Pontryagin dual of a compact group is discrete and vice versa. Thus the pairing $\mathrm{Gal}(L/K) \times A \to \mu_n$ identifies the two groups with the Pontryagin dual groups of each other.

We only explain why the map $A \to \mathrm{Gal}(L/K)^\vee$ induced by the pairing is an isomorphism in the case when both A and $\mathrm{Gal}(L/K)$ are finite. We have a short exact sequence of $\mathrm{Gal}(L/K)$-modules:

$$1 \to \mu_n \to L^\times \xrightarrow{x \mapsto x^n} (L^\times)^n \to 1.$$

We obtain the long exact sequence:

$$1 \to \mu_n \to K^\times \xrightarrow{x \mapsto x^n} K^\times \cap (L^\times)^n \xrightarrow{\delta} \mathbf{H}^1(\mathrm{Gal}(L/K), \mu_n) \to \mathbf{H}^1(\mathrm{Gal}(L/K), L^\times) \to \cdots$$

By Hilbert 90, $\mathbf{H}^1(\mathrm{Gal}(L/K), L^\times)$ is trivial. Since $\mathrm{Gal}(L/K)$ acts trivially on μ_n, we have $\mathbf{H}^1(\mathrm{Gal}(L/K), \mu_n) \cong \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)$. The cokernel of the map before δ is exactly A. Thus δ induces an isomorphism $A \xrightarrow{\sim} \mathrm{Gal}(L/K)^\vee$. Tracing the definitions we see that this isomorphism agrees with the map induced by the pairing $\mathrm{Gal}(L/K) \times A \to \mu_n$.

The following lemma will also enter the proof of Theorem 2.4.2.

Lemma 2.4.6 (Computation of local power index)**.** *Let F be a local field (archimedean or non-archimedean). Let n be a positive integer not divisible by the characteristic of F, and assume that $F \supset \mu_n$. Then $[F^\times : (F^\times)^n] = n^2/\|n\|_F$, and in the non-archimedean case we have $[\mathcal{O}_F^\times : (\mathcal{O}_F^\times)^n] = n/\|n\|_F$. Here $\|\cdot\|_F$ denotes the normalized absolute value.*

Proof. In the archimedean case, if $F = \mathbb{C}$ then we always have $[F^\times : (F^\times)^n] = 1 = n^2/\|n\|_F$. If $F = \mathbb{R}$, then since F contains all n-th roots of unity we have $n \in \{1, 2\}$. One then directly verifies the statement.

Assume that F is non-archimedean. Since $F^\times \cong \mathbb{Z} \times \mathcal{O}_F^\times$, it suffices to prove the formula for $[\mathcal{O}_F^\times : (\mathcal{O}_F^\times)^n]$. Let $G = \mathbb{Z}/n$. For any abelian group M, if we view M as a G-module with trivial action, then the Herbrand quotient is

$$h_n(M) = \frac{\#\widehat{\mathbf{H}}^0(G, M)}{\#\widehat{\mathbf{H}}^1(G, M)} = \frac{[M : nM]}{\#M[n]}$$

where $M[n] = \ker(n : M \to M)$. Since $\mathcal{O}_F^\times[n] = \mu_n$, we have $[\mathcal{O}_F^\times : (\mathcal{O}_F^\times)^n] = nh_n(\mathcal{O}_F^\times)$. It remains to show that

$$h_n(\mathcal{O}_F^\times) = \|n\|_F^{-1}.$$

If F has characteristic zero, then for sufficiently large i we have an isomorphism of abelian groups $(1 + \mathfrak{m}_F^i, \times) \cong (\mathcal{O}_F, +)$ via the logarithm map. Since the left hand side is a finite index subgroup of $\mathcal{O}_F^\times$, we get

$$h_n(\mathcal{O}_F^\times) = h_n(\mathcal{O}_F) = [\mathcal{O}_F : n\mathcal{O}_F] = \|n\|_F^{-1},$$

done.

If F has positive characteristic, then n is a non-zero element of the constant field of F, so $\|n\|_F = 1$. It suffices to prove that $h_n(1 + \mathfrak{m}_F) = 1$. For this, by Lemma 1.21.2, it suffices to prove that $\mathbf{H}^q(G, 1 + \mathfrak{m}_F^i/1 + \mathfrak{m}_F^{i+1}) = 0$ for $q = 1, 2$ and all $i \geq 1$. On the one hand, this group is killed by n, and on the other hand, $1 + \mathfrak{m}_F^i/1 + \mathfrak{m}_F^{i+1} \cong k_F$ is killed by $|k_F|$, which is a power of the characteristic of F and is hence coprime to n. The desired vanishing follows. □

Proof of Theorem 2.4.2 for characteristic not p. In view of Lemma 2.4.3, we assume that $K \supset \mu_p$. We shall show the stronger statement: For every finite Kummer extension L/K with respect to p, we have $[C_K : \mathrm{N}_{L/K} C_L] \leq [L : K]$. We follow [CF+67, §VII.9].

Write G for $\mathrm{Gal}(L/K)$. By Kummer theory L is of the form $K(\sqrt[p]{a_1}, \ldots, \sqrt[p]{a_k})$ for some $a_1, \ldots, a_k \in K^\times$. Let S be a finite subset of V_K satisfying the following conditions:

(1) S contains all archimedean places of K and all non-archimedean places of K which ramify in L.
(2) For every $v \in V_K - S$, we have $\{p, a_1, \ldots, a_k\} \subset \mathcal{O}_{K_v}^\times$.[6]
(3) We have $\mathbb{A}_K^\times = K^\times \mathbb{A}_{K,S}^\times$ (see the discussion below Fact 2.3.4).

Note that for any finite subset $T \subset V_K - S$ such that all elements of T are split in L, the group

$$E_{S,T} := \prod_{v \in S} (K_v^\times)^p \times \prod_{v \in T} K_v^\times \times \prod_{v \in V_K - (S \cup T)} \mathcal{O}_{K_v}^\times$$

is contained in the image of $\mathrm{N}_{L:K} : \mathbb{A}_L^\times \to \mathbb{A}_K^\times$. Indeed, for every $v \in V_K$ and $w \in V_L$ above v, we have $(K_v^\times)^p \subset \mathrm{N}_{L_w/K_v} L_w^\times$, since by local class field theory we have $K_v^\times / \mathrm{N}_{L_w/K_v} L_w^\times \cong \mathrm{Gal}(L_w/K_v)$ and this group is killed by p. If v is split in L, then $L_w = K_v$ and trivially

[6] This actually implies that v is unramified in L. Hence the requirement in (1) that S contains all ramified non-archimedean places is redundant. For the current proof we do not need to know this.

we have $K_v^\times = \mathrm{N}_{L_w/K_v} L_w^\times$. If v is non-archimedean and unramified in L, we have $\mathcal{O}_{K_v}^\times \subset \mathrm{N}_{L_w/K_v} \mathcal{O}_{L_w}^\times$ (see Remark 1.21.4).

Therefore, if $\bar{E}_{S,T}$ denotes the image of $E_{S,T}$ in C_K, then

$$[C_K : \mathrm{N}_{L/K} C_L] \leq [C_K : \bar{E}_{S,T}].$$

In the following we shall construct T such that $[C_K : \bar{E}_{S,T}] \leq [L : K]$.

Let $M = K(\sqrt[p]{x}, x \in \mathcal{O}_{K,S}^\times)$. Thus

$$\mathrm{Gal}(M/K)^\vee \cong \mathcal{O}_{K,S}^\times K^\times/(K^\times)^p \subset K^\times/(K^\times)^p.$$

Note that $\mathcal{O}_{K,S}^\times \cap (K^\times)^p = (\mathcal{O}_{K,S}^\times)^p$. Hence $\mathcal{O}_{K,S}^\times K^\times/(K^\times)^p \cong \mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^p$, and this is isomorphic to $(\mathbb{Z}/p)^{|S|}$ by Dirichlet's unit theorem and the fact that $\mathcal{O}_{K,S}^\times \supset \mu_n$. In particular $[M : K] = p^{|S|}$.

Since $L = K(\sqrt[p]{a_1}, \ldots, \sqrt[p]{a_k})$ and each $a_i \in \mathcal{O}_{K,S}^\times$, we have $L \subset M$. Let $[M : L] = p^t$. Thus $\mathrm{Gal}(M/L) \cong (\mathbb{Z}/p)^t$. Since this is an $\mathbb{F}_p$-vector space, by Corollary 2.3.6 we can find $w_1, \ldots, w_t \in V_L$ not lying above S such that every w_i is unramified in M and $\{\mathrm{Frob}(M/w_1), \ldots, \mathrm{Frob}(M/w_t)\}$ is an $\mathbb{F}_p$-basis of $\mathrm{Gal}(M/L)$. Let v_i be the place of K below w_i. Then the v_i's are distinct and none of them lie in S. We have $\mathrm{Frob}(M/w_i) = \mathrm{Frob}(M/v_i)^{f(w_i/v_i)}$. But every non-trivial element of $\mathrm{Gal}(M/K)$ has order p and $f(w_i/v_i)$ is a power of p (since it divides $[L : K]$), so we must have $f(w_i/v_i) = 1$, i.e., v_i splits in L. Let $T = \{v_1, \ldots, v_t\}$. We have seen that T is a set disjoint from S and consists of places which split in L. It remains to show that

$$[C_K : \bar{E}_{S,T}] \leq [L : K].$$

In general, if A, B, C are subgroups of an abelian group and $A \supset B$, then

$$[AC : BC][A \cap C : B \cap C] = [A : B].$$

Hence

$$[C_K : \bar{E}_{S,T}] = [\mathbb{A}_K^\times : K^\times E_{S,T}] = [K^\times \mathbb{A}_{K,S\cup T}^\times : K^\times E_{S,T}] = \frac{[\mathbb{A}_{K,S\cup T}^\times : E_{S,T}]}{[\mathcal{O}_{K,S\cup T}^\times : K^\times \cap E_{S,T}]}$$

where for the second equality we use condition (3) satisfied by S. By Lemma 2.4.6, the numerator is

$$[\mathbb{A}_{K,S\cup T}^\times : E_{S,T}] = \prod_{v\in S} [K_v^\times : (K_v^\times)^p] = \prod_{v\in S} \frac{p^2}{\|p\|_v} = p^{2|S|} = [M : K]^2,$$

where for the last equality we use condition (2) satisfied by S and the product formula.

It remains to show that $K^\times \cap E_{S,T} = (\mathcal{O}_{K,S\cup T}^\times)^p$. For then by Dirichlet's unit theorem as before we can calculate the denominator:

$$[\mathcal{O}_{K,S\cup T}^\times : K^\times \cap E_{S,T}] = [\mathcal{O}_{K,S\cup T}^\times : (\mathcal{O}_{K,S\cup T}^\times)^p] = p^{|S\cup T|} = [M : K][M : L],$$

and it follows that

$$[C_K : \bar{E}_{S,T}] = \frac{[M : K]^2}{[M : K][M : L]} = [L : K],$$

as desired.

Clearly we have $K^\times \cap E_{S,T} \supset (\mathcal{O}_{K,S\cup T}^\times)^p$. The reverse containment follows from the following claim and Proposition 2.4.7 below.

Claim: the map $\mathcal{O}_{K,S}^\times \to \prod_{v\in T} \mathcal{O}_{K_v}^\times/(\mathcal{O}_{K_v}^\times)^p$ is surjective.

Proof of the claim. Let Φ denote the kernel of the map. We first check that $\Phi = \mathcal{O}_{K,S}^\times \cap (L^\times)^p$. Let $a \in \mathcal{O}_{K,S}^\times \cap (L^\times)^p$. For each $v \in T$, since v splits in L, for any place w of L above v we have $a \in (L^\times)^p \subset (L_w^\times)^p = (K_v^\times)^p$. Hence $a \in \Phi$. Conversely, let $a \in \Phi$. By the construction of M, there exists $\sqrt[p]{a} \in M$. It suffices to show that $\sqrt[p]{a}$ is fixed by $\mathrm{Gal}(M/L)$, and for this its suffices that $\mathrm{Frob}(M/w_i)$ fixes $\sqrt[p]{a}$ for all $1 \le i \le t$, since these Frobenius elements generate $\mathrm{Gal}(M/L)$. But $a \in (\mathcal{O}_{K_{v_i}}^\times)^p = (\mathcal{O}_{L_{w_i}}^\times)^p$ since v_i splits in L, so $\sqrt[p]{a} \in L_{w_i}$ and it is fixed by $\mathrm{Frob}(M/w_i)$.

Since $\Phi = \mathcal{O}_{K,S}^\times \cap (L^\times)^p$, we have

$$[\mathcal{O}_{K,S}^\times : \Phi] = [\mathcal{O}_{K,S}^\times L^\times : (L^\times)^p] = |\mathrm{Gal}(M/L)^\vee| = p^t.$$

Also $\prod_{v\in T} \mathcal{O}_{K_v}^\times/(\mathcal{O}_{K_v}^\times)^p$ has cardinality $\prod_{v\in T} p/\|p\|_v = p^t$ by Lemma 2.4.6 and the assumption that $p \in \mathcal{O}_{K_v}^\times$ for all $v \notin S$. The claim is proved. □

Proposition 2.4.7. *Let n be a positive integer not divisible by $\mathrm{char}K$. Assume that $K \supset \mu_n$. Let S be a finite subset of V_K containing all archimedean places and satisfying:*

(1) *For every $v \in V_K - S$, we have $n \in \mathcal{O}_{K_v}^\times$.*
(2) *We have $\mathbb{A}_K^\times = K^\times \mathbb{A}_{K,S}^\times$.*

Let T be a finite subset of V_K disjoint from S. Assume that the map $\mathcal{O}_{K,S}^\times \to \prod_{v\in T} \mathcal{O}_{K_v}^\times/(\mathcal{O}_{K_v}^\times)^n$ is surjective. Then

$$K^\times \cap \left(\prod_{v\in S} (K_v^\times)^n \times \prod_{v\in T} K_v^\times \times \prod_{v\in V_K - S\cup T} \mathcal{O}_{K_v}^\times \right) \subset (K^\times)^n.$$

Proof. Let b be an element of the left hand side, and let $L = K(\sqrt[n]{b})$. It suffices to show that $L = K$. The extension L/K is Kummer and corresponds to the subgroup of $K^\times/(K^\times)^n$ generated by b, so it is cyclic. Thus we have the First Inequality $[C_K : \mathrm{N}_{L/K} C_L] \ge [L : K]$. It suffices to show that $\mathrm{N}_{L/K} C_L = C_K$.

Let $D = \prod_{v\in S} K_v^\times \times \prod_{v\in T} (\mathcal{O}_{K_v}^\times)^n \times \prod_{v\in V_K - S\cup T} \mathcal{O}_{K_v}^\times$. For each $v \in V_K$ and $w \in V_L$ above v, we know the following:

- If $v \in S$, then $L_w = K_v$ since $\sqrt[n]{b} \in K_v^\times$.
- If $v \in T$, then $(\mathcal{O}_{K_v}^\times)^n \subset \mathrm{N}_{L_w/K_v} L_w^\times$ since by local class field theory the latter group has index n in $K_v^\times$.
- If $v \notin S \cup T$, then since $n, b \in \mathcal{O}_{K_v}^\times$, the extension L_w/K_v is unramified. In particular, $\mathcal{O}_{K_v}^\times = \mathrm{N}_{L_w/K_v} \mathcal{O}_{L_w}^\times$.

In conclusion, we have $D \subset \mathrm{N}_{L/K} \mathbb{A}_L^\times$. It remains to show that D maps onto C_K, i.e., $\mathbb{A}_K^\times = K^\times D$. For this,

$$\mathbb{A}_K^\times/K^\times D = K^\times \mathbb{A}_{K,S}^\times/K^\times D \cong (\mathbb{A}_{K,S}^\times/D)/\mathrm{im}(\mathbb{A}_{K,S}^\times \cap K^\times) = (\prod_{v\in T} \mathcal{O}_{K_v}^\times)/\mathrm{im}(\mathcal{O}_{K,S}^\times) = 1.$$

□

Remark 2.4.8. We can take $T = \emptyset$. Then the proposition asserts that for any finite S containing the archimedean places and satisfying (1) (2), we have

$$K^\times \cap \left(\prod_{v\in S} (K_v^\times)^n \times \prod_{v\in V_K - S} \mathcal{O}_{K_v}^\times \right) \subset (K^\times)^n.$$

2.5. **The Second Inequality for bad characteristic.** We now treat the case of Theorem 2.4.2 when the degree p of L/K is equal to the characteristic of K, following [AT09, §IV.4].

We first need a replacement of Kummer theory, which is *Artin–Schreier theory*. Let K be an arbitrary field of characteristic $p > 0$. We call an algebraic extension L/K *Artin–Schreier* if it is abelian and $\mathrm{Gal}(L/K)$ is killed by p. Define the endomorphism of the additive group

$$\wp : K \to K, \quad x \mapsto x^p - x.$$

Its kernel is clearly $\mathbb{F}_p \subset K$. This map plays the analogous role as the n-th power map in Kummer theory, and $\mathbb{F}_p$ plays the analogous role as μ_n.

Fact 2.5.1 (Artin–Schreier theory)**.** *An algebraic extension L/K is an Artin–Schreier extension if and only if L is of the form $K(\wp^{-1}(A))$ for a subset A of K, where $\wp^{-1}$ denotes taking inverse image in K^s. We have a bijection*

$$\{\textit{Artin–Schreier extensions of } K \textit{ in } K^s\} \xrightarrow{\sim} \{\textit{subgroups of } K/\wp(K)\}$$

sending L/K to $(K \cap \wp(L))/K$, and the inverse map sends A to $L = K(\wp^{-1}(A))$. Assume that L/K corresponds to A under the bijection. Then we have a bi-additive pairing

$$\begin{aligned} \mathrm{Gal}(L/K) \times A &\longrightarrow \mathbb{F}_p \\ (g, a) &\longmapsto gx - x. \end{aligned}$$

Here, for each $a \in A$, we choose $x \in L$ such that $\wp(x) = \tilde{a}$ and $\tilde{a} \in K$ maps to a. The pairing is independent of choices, and identifies $\mathrm{Gal}(L/K)$ (with the Krull topology) and A (with the discrete topology) with the Pontryagin dual of each other (cf. Remark 2.4.5). In particular, $[L : K]$ is finite if and only if A is finite, and in this case we have $[L : K] = |A|$.

We explain why an extension of the form $L = K(\wp^{-1}(A))$ is Artin–Schreier. Clearly it is normal. To see it is separable, note that for any $a \in K$, the polynomial $f(X) = X^p - X - a$ satisfies $f'(X) = -1$, and clearly it has a root in K if and only if it splits in K (as all roots differ from each other by $\mathbb{F}_p$). Hence it suffices to see that $f(X)$ is irreducible over K when it has no root over K. Suppose it has a proper factor $(X - x_1) \cdots (X - x_r)$ over K, with $2 \leq r < p$. Then the subleading coefficient of this factor is $-(x_1 + \cdots + x_r) \in -rx_1 + \mathbb{F}_p$, a contradiction since $r \in K^\times$ and $x_1 \notin K$. Thus we have seen that L/K is Galois. To see $\mathrm{Gal}(L/K)$ is abelian and killed by p, it suffices to note that the pairing $\mathrm{Gal}(L/K) \times A \to \mathbb{F}_p$ has no kernel in $\mathrm{Gal}(L/K)$ and so $\mathrm{Gal}(L/K)$ is a subgroup of $\mathrm{Hom}(A, \mathbb{F}_p)$.

We now explain why the map $A \to \mathrm{Gal}(L/K)^\vee = \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{F}_p)$ induced by the pairing is an isomorphism in the case when both A and $\mathrm{Gal}(L/K)$ are finite. We have a short exact sequence of $\mathrm{Gal}(L/K)$-modules:

$$1 \to \mathbb{F}_p \to L \xrightarrow{\wp} \wp(L) \to 1.$$

We obtain the long exact sequence:

$$1 \to \mathbb{F}_p \to K \xrightarrow{\wp} K \cap \wp(L) \xrightarrow{\delta} \mathbf{H}^1(\mathrm{Gal}(L/K), \mathbb{F}_p) \to \mathbf{H}^1(\mathrm{Gal}(L/K), L) \to \cdots$$

By Proposition 1.19.1, $\mathbf{H}^1(\mathrm{Gal}(L/K), L)$ is trivial. Since $\mathrm{Gal}(L/K)$ acts trivially on $\mathbb{F}_p$, we have $\mathbf{H}^1(\mathrm{Gal}(L/K), \mathbb{F}_p) \cong \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{F}_p)$. The cokernel of the map before δ is exactly A. Thus δ induces an isomorphism $A \xrightarrow{\sim} \mathrm{Gal}(L/K)^\vee$. Tracing the definitions we see that this isomorphism agrees with the map induced by the pairing $\mathrm{Gal}(L/K) \times A \to \mathbb{F}_p$.

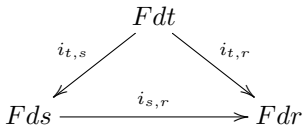
We now discuss *differentials and residues*, with the ultimate goal of stating a duality theorem (Fact 2.5.12) for the global function field K, which is a deep result entering the proof of the Second Inequality as a black box. The main reference being cited in [AT09]

for this material is Artin's book [Art06]. A more modern reference is [Ser88]; see especially Chapter II, which also contains a bibliographic note at the end.

Let F be a local function field of characteristic p, with residue field $k = \mathbb{F}_q$. Recall that for each choice of uniformizer $t \in F$, we have a canonical isomorphism $k(\!(t)\!) \xrightarrow{\sim} F$ sending a Laurent series to its convergent value in F. For such t, consider the 1-dimensional F-vector space Fdt, where dt is a formal symbol and is a basis of the vector space. If s is another uniformizer, we define an F-vector space isomorphism

$$i_{t,s} : Fdt \xrightarrow{\sim} Fds, \quad dt \mapsto \frac{dt}{ds} ds.$$

Here, t is a Laurent series $t(s) \in F \cong k(\!(s)\!)$ (in fact a power series without constant term), and $\frac{dt}{ds}$ denotes term-wise differentiation, i.e., if $t = \sum_{n\geq 1} a_n s^n$ then $\frac{dt}{ds} = \sum_{n\geq 1} n a_n s^{n-1}$. If t, s, r are three uniformizers, then we have a commutative diagram



Thus we can compatibly identify the F-vector spaces Fdt for *all* choices of uniformizers t, and we denote the resulting space by $\hat{\Omega}_{F/k}$. We have a canonical k-linear map

$$d : F \to \hat{\Omega}_{F/k}, \quad f \mapsto \frac{df}{dt} dt,$$

where t is any uniformizer, and $\frac{df}{dt}$ again denotes term-wise differentiation of the Laurent series $f = f(t) \in F \cong k(\!(t)\!)$. This map is independent of the choice of t.

Exercise 2.5.2. In this exercise we show how to abstractly characterize the pair

$$(\hat{\Omega}_{F/k},\ d : F \to \hat{\Omega}_{F/k}).$$

Show that the $\mathcal{O}_F$-submodule $\mathcal{O}_F dt$ of $\hat{\Omega}_{F/k}$ is independent of the choice of a uniformizer t. Denote it by $\hat{\Omega}_{\mathcal{O}_F/k}$. Show that d restricts to a map $\mathcal{O}_F \to \hat{\Omega}_{\mathcal{O}_F/k}$, and the pair

$$(\hat{\Omega}_{\mathcal{O}_F/k},\ d : \mathcal{O}_F \to \hat{\Omega}_{\mathcal{O}_F/k})$$

is characterized by the following universal property:

- The $\mathcal{O}_F$-module $\hat{\Omega}_{\mathcal{O}_F/k}$ is $\mathfrak{m}_F$-adically complete, (i.e., the natural map $\hat{\Omega}_{\mathcal{O}_F/k} \to \varprojlim_{n\geq 1} \hat{\Omega}_{\mathcal{O}_F/k}/\mathfrak{m}_F^n \hat{\Omega}_{\mathcal{O}_F/k}$ is an isomorphism), and d is a k-linear map satisfying $d(fg) = fdg + gdf$;
- For any pair (B, d_B) consisting of an $\mathfrak{m}_F$-adically complete $\mathcal{O}_F$-module M and a k-linear map $d_B : \mathcal{O}_F \to M$ satisfying $d_B(fg) = f d_B g + g d_B f$, there is a unique k-linear map $\phi : \hat{\Omega}_{\mathcal{O}_F/k} \to B$ such that $d_B = \phi \circ d$.

Then show that we have a canonical identification $\hat{\Omega}_{F/k} \cong F \otimes_{\mathcal{O}_F} \hat{\Omega}_{\mathcal{O}_F/k}$, and moreover $d : F \to \hat{\Omega}_{F/k}$ is given by $d(f/g) = g^{-2} \otimes (gdf - fdg)$ for $f, g \in \mathcal{O}_F, g \neq 0$.

Definition 2.5.3. For any element $\omega \in \hat{\Omega}_{F/k}$, choose a uniformizer t and write $\omega = (\sum_{i\geq n} a_i t^i) dt$, with $a_i \in k$. Define the *residue* of ω to be $a_{-1} \in k$. We denote it by $\operatorname{Res} \omega$.

Lemma 2.5.4. *The definition of the residue is independent of the choice of uniformizer.*

Proof. Let s be another uniformizer. Then

$$\omega = (\sum_{i\geq n} a_i t^i)dt = (\sum_{i\geq n} a_i t(s)^i)\frac{dt}{ds}ds.$$

Clearly the coefficient of s^{-1} in $(\sum_{i\geq 0} a_i t(s)^i)\frac{dt}{ds}$ is 0 (since $t(s)$ is a power series). Hence we may assume $\omega = t^{-n}dt$ for some $n \geq 1$. We need to show that the coefficient of s^{-1} in $t(s)^{-n}\frac{dt}{ds}$ is 1 for $n = 1$ and 0 for $n \geq 2$.

Write $t = su^{-1}$, with $u \in \mathcal{O}_F^\times$. Then

$$t(s)^{-n}\frac{dt}{ds} = s^{-n}u^n\frac{u - s\frac{du}{ds}}{u^2}.$$

Let

$$f(s) = u^n\frac{u - s\frac{du}{ds}}{u^2}.$$

Thus we need to show that the coefficient of s^{n-1} is f is 1 for $n = 1$ and 0 for $n \geq 2$. For $n = 1$, we have $f(s) = 1 - su^{-1}\frac{du}{ds}$ and so $f(0) = 1$, as desired. For $n \geq 2$, in anticipation of a difficulty cased by positive characteristic, we lift the problem to characteristic zero in the following way: Consider $U(s) = b_0 + b_1 s + b_2 s^2 + \cdots \in R[\![s]\!]$, where $R = \mathbb{Z}[b_0, b_1, \cdots]$ with the b_i's being formal variables. Define

$$F(s) = U^{n-1} - U^{n-2}s\frac{dU}{ds} \in R[\![s]\!].$$

Clearly U and F specialize to u and f, i.e., if we map R to k sending b_i to the coefficients of u, then the induced map $R[\![s]\!] \to k[\![s]\!]$ sends U to u and F and f. It suffices to prove that the coefficient $A \in R$ of s^{n-1} in $F(s)$ is 0. We have

$$(n-1)!A = \left.\frac{d^{n-1}}{ds^{n-1}}\right|_{s=0} F(s) = \left.\frac{d^{n-1}}{ds^{n-1}}\right|_{s=0} (U^{n-1}) - (n-1)\left.\frac{d^{n-2}}{ds^{n-2}}\right|_{s=0} (U^{n-2}\frac{dU}{ds}).$$

This is zero since

$$(n-1)(U^{n-2}\frac{dU}{ds}) = \frac{d}{ds}(U^{n-1}).$$

Hence $A = 0$ since multiplication by $(n-1)!$ is injective on R. (The last argument does not work for k in place of R.) □

Exercise 2.5.5. Show that the pairing $\hat{\Omega}_{F/k} \times F \to k, (\omega, f) \mapsto \mathrm{Res}(f\omega)$ induces an isomorphism from $\hat{\Omega}_{F/k}$ to the space of continuous k-linear maps $F \to k$ (where F has the usual non-archimedean topology and k has the discrete topology).

If t, s are uniformizers of F, clearly $dt/ds \in \mathcal{O}_F^\times$. Hence for any $\omega = fdt \in \hat{\Omega}_{F/k} = Fdt$, the integer $\mathrm{ord}(f)$ depends only on ω, not on the choice of t. We define it to be the order of ω, denoted by $\mathrm{ord}(\omega)$.

Now let K be a global function field of characteristic p, with field of constants k (i.e., k is the algebraic closure of $\mathbb{F}_p$ in K). Recall that K is of transcendence degree 1 over k, so one can choose (non-canonically) an element $t \in K$ which is transcendental over k, and realize K as a finite extension of the field of rational functions $k(t)$. This point of view is important for the proofs of some of the facts discussed below, but we will not make too much use of it.

Let $(\Omega_{K/k}, d)$ be the usual module of differentials, which is characterized as the initial object among pairs (B, d_B) where B is a K-vector space and d_B is a k-linear map $K \to B$ satisfying $d_B(fg) = fd_Bg + gd_Bf$.

Fact 2.5.6. *The following statements hold.*

(1) *The K-vector space $\Omega_{K/k}$ is one-dimensional.*
(2) *Let $v \in V_K$, and write k_v for the residue field of K_v. By the universal property of $(\Omega_{K/k}, d)$, there is a unique map $i : \Omega_{K/k} \to \hat{\Omega}_{K_v/k_v}$ making the following diagram commute:*

$$\begin{array}{ccc} K & \hookrightarrow & K_v \\ \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} \\ \Omega_{K/k} & \xrightarrow{i} & \hat{\Omega}_{K_v/k_v} \end{array}$$

The map i is injective. In particular, if $t \in K$ is a local uniformizer at v (such t clearly exists), then $dt \in \Omega_{K/k}$ is a K-basis of $\Omega_{K/k}$.
(3) *Let $\omega \in \Omega_{K/k}$. Then for almost all $v \in V_K$, we have $\mathrm{ord}_v(\omega) = 0$, i.e., the image of ω in $\hat{\Omega}_{K_v/k_v}$ is of the form $f_v dt_v$ for $f_v \in \mathcal{O}_{K_v}^\times$ and t_v a local uniformizer.*
(4) *(Theorem of Residue.) Let $\omega \in \Omega_{K/k}$. For $v \in V_K$, denote by $\mathrm{Res}_v(\omega) \in k_v$ the residue of the image of ω in $\hat{\Omega}_{K_v/k_v}$. By (3), this vanishes for almost all v. We have*

$$\sum_{v \in V_K} \mathrm{Tr}_{k_v/k} \mathrm{Res}_v(\omega) = 0.$$

Remark 2.5.7. The above notions have the following geometric interpretations. Let X be the smooth projective geometrically connected curve over k such that $K = k(X)$. Then $\Omega_{K/k}$ is the space of global meromorphic differentials on X. The set V_K of all places of K is identified with the set of closed points of X. For $v \in V_K$, $\hat{\Omega}_{K_v/k_v}$ is the space of meromorphic differentials defined on the formal disk centered at v which are holomorphic away from v. The map $i : \Omega_{K/k} \to \Omega_{K_v/k_v}$ has the interpretation of restricting a global meromorphic differential to a local formal disk. Fact (3) above corresponds to the fact that any global differential has only finitely many zeros and poles.

Let $t \in K$ be a uniformizer at some $v \in V_K$. By (1) and (2) in Fact 2.5.6, for any $f \in K$ there is $g \in K$ such that $df = g dt$, and moreover g can be computed as $g = df/dt$ in $K_v \cong k_v((t))$. As a consequence, taking derivative in $k_v((t))$ preserves the subfield $K \subset k_v((t))$. In the following exercise we directly prove this.

Exercise 2.5.8. Let k be a finite (or more generally, perfect) field.

(1) Show that the extension $k((t))/k(t)$ is separable. Hint: Suppose $f \in k((t))$ is algebraic and non-separable over $k(t)$. Let $F(X) \in k(t)[X]$ be the minimal polynomial of f. Let $f_1(t) = f(t^p) \in k((t))$. Construct a polynomial $F_1(X) \in k(t)[X]$ of smaller degree than F such that $F_1(f_1) = 0$. Then show the following fact: If $a_0(t), \dots, a_n(t) \in k[t]$ are such that

$$\sum_i a_i(t) f_1(t)^i = 0,$$

then the same equation still holds if we modify each $a_i(t)$ by discarding all terms t^j for j coprime to p.
(2) Let $f \in k((t))$ be algebraic over $k(t)$. Then df/dt is also algebraic over $k(t)$, and more precisely $df/dt \in k(t)(f)$. (Hint: you should use the conclusion of (1).)

Exercise 2.5.9. Let $s \in K$ be transcendental over k, so K is a finite extension of $k(s)$. Show that the extension $K/k(s)$ is separable if and only if $ds \neq 0$ in $\Omega_{K/k}$. (Hint: for the "only if" direction, use Fact 2.5.6 (2) and the previous exercise.)

Example 2.5.10. Let k be a finite field of characteristic $p \neq 2$. Let $P(X) \in k[X]$ and assume that $P(X)$ is not a square in $k[X]$. Let $K = k(X)[Y]/(Y^2 - P(X))$. Then K is a global function field (but the field of constants may be larger than k). Suppose there is an element $a \in k$ such that $P(a) \neq 0$. Let $t = X - a$. Then

$$Y^2 = P(t+a) = c_0 + c_1 t + \cdots + c_n t^n,$$

with $c_i \in k, c_0 \neq 0$. Let

$$S(u) = \sum_{i=0}^{\infty} \binom{1/2}{i} u^i \in k((u)).$$

Then $S(u)^2 = 1 + u$, and in particular by differentiating both sides we have $S'(u) = (2S(u))^{-1}$. Let $k' = k(\sqrt{c_0})$, which is either k or a quadratic extension of k. We have a k-algebra embedding $K \hookrightarrow k'((t))$ sending X to $t+a$ and sending Y to $\sqrt{c_0} S(\frac{c_1}{c_0} t + \cdots + \frac{c_n}{c_0} t^n)$, which is indeed a well-defined element of $k'((t))$. Pulling back the valuation on $k'((t))$ to K, we obtain a place v of K, and the element $t = X - a \in K$ is a local uniformizer at v.

For any $f \in K$, $df \in \Omega_{K/k}$ is a K-multiple of dt, and the multiplier in K can be computed as df/dt inside $k((t))$. For instance,

$$\frac{dY}{dt} = \sqrt{c_0} S'(\frac{c_1}{c_0} t + \cdots + \frac{c_n}{c_n} t^n) c_0^{-1} (c_1 + 2c_2 t + \cdots + n c_n t^{n-1}) = (2Y)^{-1} (c_1 + 2c_2 t + \cdots + n c_n t^{n-1}),$$

which is indeed an element of K.

Example 2.5.11. Let k be a finite field and $K = k(t)$, the function field of $\mathbb{P}^1$ over k. Recall that the places of K correspond to non-zero prime ideals of $k[t]$ and ∞. If v corresponds to a non-zero prime ideal of $k[t]$, or equivalently a monic irreducible polynomial $m(t) \in k[t]$, then $\operatorname{ord}_v(f(t)/g(t))$ is the exponent of $m(t)$ in the irreducible factorization of $f(t)$ minus the similar number for $g(t)$, for all $f(t), g(t) \neq 0 \in k[t]$. If $v = \infty$, then $\operatorname{ord}_v(f(t)/g(t)) = \deg g - \deg f$.

Consider $\omega = dt \in \Omega_{K/k}$. If v corresponds to an irreducible $m(t) \in k[t]$, then $s_v := m(t) \in K$ is a uniformizer at v, and in $K_v \cong k_v((s_v))$ we have

$$\frac{dt}{ds_v} = (\frac{ds_v}{dt})^{-1} = (m'(t))^{-1} \in K^\times.$$

(Note that $m'(t) \neq 0$ since $m(t)$ is irreducible over k and k is perfect.) Moreover, $m'(t)$ is coprime to $m(t)$ in $k[t]$, so $m'(t)^{-1} \in \mathcal{O}_{K_v}^\times$. Hence $\operatorname{Res}_v dt = 0$.

For $v = \infty$, a uniformizer is $s = t^{-1}$. We have

$$\frac{dt}{ds} = -s^{-2},$$

so $\operatorname{Res}_v dt = 0$. We have seen that $\omega = dt$ has zero residue everywhere. Note that $\sum_v \operatorname{ord}_v \omega = -2$. This property is independent of the choice of ω, since a different non-zero element of $\Omega_{K/k}$ differs by multiplication by some $f \in K^\times$, and by the product formula we have $\sum_v \operatorname{ord}_v(f) = 0$.

We can now state the duality theorem for the global function field K. Define the pairing

$$\langle \cdot, \cdot \rangle : \Omega_{K/k} \times \mathbb{A}_K \longrightarrow k, \quad (\omega, (a_v)_v) \longmapsto \sum_{v \in V_K} \operatorname{Tr}_{k_v/k} \operatorname{Res}_v(a_v \omega).$$

By Fact 2.5.6 (3), this is a finite sum. By Fact 2.5.6 (4), this pairing kills $K \subset \mathbb{A}_K$. It is easy to see that the pairing induces a map

$$\Omega_{K/k} \longrightarrow \{\text{continuous } k\text{-linear maps } \mathbb{A}_K \to k\}.$$

Fact 2.5.12 (The duality theorem)**.** *The above map is an isomorphism.*

Exercise 2.5.13. Prove injectivity. (Surjectivity is the deep part.)

Corollary 2.5.14. *Let $a = (a_v)_v \in \mathbb{A}_K$ be such that $\langle \omega, a\rangle = 0$ for all $\omega \in \Omega_{K/k}$. Then $a \in K$.*

Proof. Fix a non-zero $\omega_0 \in \Omega_{K/k}$. The map $\mathbb{A}_K \to k, b \mapsto \langle \omega_0, ab\rangle$ is clearly continuous and k-linear. It kills K, since for $b \in K$ we have $\langle \omega_0, ab\rangle = \langle b\omega_0, a\rangle = 0$ by the hypothesis on a. Thus there exists $\omega_1 \in \Omega_{K/k}$ such that $\langle \omega_0, ab\rangle = \langle \omega_1, b\rangle$ for all $b \in \mathbb{A}_K$. Write $\omega_1 = \lambda\omega_0$. Then we have

$$\langle \omega_0, (\lambda - a)b\rangle = 0, \quad \forall b \in \mathbb{A}_K.$$

For any $v \in V_K$ and $b_v \in K_v$, we can choose $b \in \mathbb{A}_K$ such that the component of b at v is b_v and such that $\mathrm{ord}_w((\lambda - a_w)b_w\omega_0) \geq 0$ for all $w \in V_K - \{v\}$, because $\mathrm{ord}_w((\lambda - a_w)\omega_0) < 0$ only for finitely many w (by Fact 2.5.6 (3)). Thus we conclude that for arbitrary $b_v \in K_v$, we have $\mathrm{Tr}_{k_v/k} \mathrm{Res}_v(\lambda - a_v)b_v\omega_0 = 0$. If $a_v \neq \lambda$, then we have $\mathrm{Tr}_{k_v/k} \mathrm{Res}_v c\omega_0 = 0$ for all $c \in K_v$, which is clearly a contradiction since we can arrange $\mathrm{Res}_v c\omega_0$ to be an arbitrary element of k_v. Hence $a_v = \lambda$. Since this holds for all v, we have $a = \lambda \in K$. □

In the proof of the Second Inequality, we need to consider a different pairing closely related to $\langle \cdot, \cdot \rangle$. Let $v \in V_K$. Note that the formation of "log differential" $K_v^\times \to \hat{\Omega}_{K_v/k_v}, f \mapsto f^{-1}df$ is a group homomorphism. We define the local pairing:

$$\phi_v : K_v \times K_v^\times \longrightarrow \mathbb{F}_p, \quad (x, y) \longmapsto \mathrm{Tr}_{k_v/\mathbb{F}_p} \mathrm{Res}(xy^{-1}dy).$$

This is a bi-additive map.

Lemma 2.5.15. *The following statements hold.*

1. *If $x \in \mathcal{O}_{K_v}$ is such that $\phi_v(x, t) = 0$ for a uniformizer t, then $x \in \wp(K_v)$.*
2. *For any $x \in \wp(K_v)$, we have $\phi_v(x, y) = 0$ for all $y \in K_v^\times$.*

Proof. (1) By assumption, the constant term of $x = x(t) \in \mathcal{O}_{K_v} \cong k_v[\![t]\!]$ is in the kernel of $\mathrm{Tr}_{k_v/\mathbb{F}_p}$. By Exercise 2.5.16 below, we have $x = b^p - b + a_1t + a_2t^2 + \cdots$ for $b, a_i \in k_v$. Write x_+ for $a_1t + a_2t^2 + \cdots$. Since $x_+ \in \mathfrak{m}_{K_v}$, the infinite series $-(x_+ + x_+^p + x_+^{p^2} + \cdots)$ converges to an element $z \in K_v$. Clearly $z^p - z = x_+$. Hence $x = \wp(b + z)$.

(2) Exercise. □

Exercise 2.5.16. For any finite field $\mathbb{F}_q \supset \mathbb{F}_p$, we have $\ker(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}) = \wp(\mathbb{F}_q)$. (Prove this either by counting or using cohomology.)

Exercise 2.5.17. Prove part (2) of Lemma 2.5.15 in the following steps.

1. By bi-additivity, we may assume that y is either in $k_v^\times$, or a uniformizer, or in $1 + \mathfrak{m}_{K_v}$. Prove in the first two cases.
2. Let t be a uniformizer. Show that every element of $1 + \mathfrak{m}_{K_v}$ can be written as an infinite product $\prod_{i=1}^\infty (1 + c_it^i)$, with $c_i \in k_v$. Show that ϕ_v is continuous in the second variable, and hence reduce to the case where $y = 1 + ct^i$ for some $i \geq 1$.
3. Show that ϕ_v is continuous in the first variable, and hence reduce to the case where $x = \wp(at^n) = a^pt^{pn} - at^n$ for some $a \in k_v, n \in \mathbb{Z}$.
4. For x and y as above, show that $\phi_v(x, y) = 0$. (Expand $(1 + ct^i)^{-1}$ in a geometric series.)

Now define the global pairing

$$\phi : K \times \mathbb{A}_K^\times \longrightarrow \mathbb{F}_p, \quad (x, (a_v)_v) \longmapsto \sum_v \phi_v(x, a_v).$$

Note that $\phi_v(x, a_v) = 0$ if $x \in \mathcal{O}_{K_v}$ and $a_v \in \mathcal{O}_{K_v}^\times$, so the sum is finite. Clearly ϕ is bi-additive.

Theorem 2.5.18. *The kernel in K of the pairing ϕ is $\wp(K)$. The kernel in $\mathbb{A}_K^\times$ of the pairing ϕ is $K^\times(\mathbb{A}_K^\times)^p$. The pairing ϕ identifies the discrete group $K/\wp(K)$ and the compact group $\mathbb{A}_K^\times/(K^\times(\mathbb{A}_K^\times)^p) \cong C_K/C_K^p$ with the Pontryagin dual of each other.*

Remark 2.5.19. Recall that the kernel C_K^1 of the idele norm $C_K \to |k|^{\mathbb{Z}}$ is compact. It easily follows that C_K/C_K^p is compact.

Proof. We only show the first two statements, and leave the last statement as exercise.

Suppose $x \in K$ lies in the kernel of the pairing ϕ. For every $v \in V_K$ such that $x \in \mathcal{O}_{K_v}$, we can choose an idele $a = (a_w)_w$ such that $a_w = 1$ for $w \neq v$ and a_v is a uniformizer in K_v. Then $\phi(x, a) = \phi_v(x, a_v) = 0$. By Lemma 2.5.15 (1), we have $x \in \wp(K_v)$. In particular, v splits in the Artin–Schreier extension $K(\wp^{-1}(x))/K$. Since this holds for infinitely many v, by Corollary 2.3.6 we have $K(\wp^{-1}(x)) = K$, i.e., $x \in \wp(K)$.

Conversely, $\wp(K) \subset K$ lies in the kernel of ϕ by Lemma 2.5.15 (2).

Suppose $a \in \mathbb{A}_K^\times$ lies in the kernel of ϕ. Fix $v_0 \in V_K$ and $t \in K$ to be a uniformizer at v_0. Then dt is a K-basis of $\Omega_{K/k}$ and a K_v-basis of $\hat{\Omega}_{K_v/k_v}$ for every $v \in V_K$. Define $b_v \in K_v$ by

$$b_v dt = a_v^{-1} da_v.$$

For almost all v, we have $\mathrm{ord}_v(dt) = 0$ (by Fact 2.5.6 (3)) and $\mathrm{ord}_v(a_v^{-1}da_v) \geq 0$, from which it follows that $b_v \in \mathcal{O}_{K_v}$. Hence $b = (b_v)_v$ is an element of $\mathbb{A}_K$.

For all $x \in K$, we have

$$0 = \phi(x, a) = \mathrm{Tr}_{k/\mathbb{F}_p}\big(\sum_v \mathrm{Tr}_{k_v/k} \mathrm{Res}(x a_v^{-1} da_v)\big) = \mathrm{Tr}_{k/\mathbb{F}_p}\langle x dt, b\rangle.$$

Replacing x by $x'x$ with $x' \in k$ arbitrary, we have

$$0 = \mathrm{Tr}_{k/\mathbb{F}_p}\langle x' x dt, b\rangle = \mathrm{Tr}_{k/\mathbb{F}_p}(x'\langle x dt, b\rangle).$$

Hence $\langle x dt, b\rangle = 0$. Since x is arbitrary, we have $\langle \omega, b\rangle = 0$ for all $\omega \in \Omega_{K/k}$. Thus by Corollary 2.5.14, we have $b \in K$. Now in $K_{v_0} \cong k_{v_0}((t))$, we have $b = a_{v_0}^{-1} da_{v_0}/dt$.

We use the following general fact proved in [AT09, §VI.4.a]: Let E be a field and $D : E \to E$ be an additive map satisfying $D(fg) = fD(g) + gD(f)$ and such that for every $f \in E$ there exists $n \geq 1$ such that $D^n(f) = 0$. Let F be a subfield of E stable under D. Then an element of F can be written as $y^{-1}D(y)$ for some $y \in E^\times$ if and only if it can be written as $y^{-1}D(y)$ for some $y \in F^\times$.

Applying this fact to $E = K_{v_0} = k_{v_0}((t))$, $F = K \subset E$, and $D = d/dt$ (which stabilizes K, see Exercise 2.5.8, and clearly $D^p = 0$), we conclude that $b = z^{-1}dz/dt$ for some $z \in K^\times$. It then follows that for every $v \in V_K, a_v^{-1}da_v = z^{-1}dz$. Let $c = z^{-1}a \in \mathbb{A}_K^\times$. It remains to prove that $c \in (\mathbb{A}_K^\times)^p$. For every $v \in V_K$, we have

$$\frac{dc_v}{c_v} = \frac{da_v}{a_v} - \frac{dz}{z} = 0.$$

Hence if t_v is a uniformizer in K_v, then $dc_v/dt_v = 0$, i.e., the Laurent series in t_v representing c_v is of the form $\sum_{i \geq n} e_i t_v^{pi}$, $e_i \in k_v$. Since k_v is a perfect field, this Laurent series is a p-th power, i.e., $c_v \in (K_v^\times)^p$. Hence $c \in (\mathbb{A}_K^\times)^p$ as desired.

Finally, we show that $K^\times(\mathbb{A}_K^\times)^p$ lies in the kernel of ϕ. By the theorem of residue, $K^\times$ lies in the kernel. Since the target $\mathbb{F}_p$ of ϕ is killed by p, $(\mathbb{A}_K^\times)^p$ lies in the kernel. □

Exercise 2.5.20. Prove the last statement in Theorem 2.5.18.

By Artin-Schreier theory, the Pontryagin dual of $K/\wp(K)$ is also identified with $\mathrm{Gal}(M/K)$, where M/K is the maximal Artin–Schreier extension, namely $M = K(\wp^{-1}(K))$. Thus we obtain a canonical isomorphism of topological groups

$$\Phi : C_K/C_K^p \xrightarrow{\sim} \mathrm{Gal}(M/K).$$

Unraveling the definitions, we have the following concrete characterization of Φ. Let $a \in \mathbb{A}_K^\times$ and $y = \wp^{-1}(x) \in M$ with $x \in K$. Then

$$\Phi(a)y = y + \phi(x, a).$$

We need a last preparation before proving the Second Inequality.

Lemma 2.5.21. *Let K be a global field of any characteristic. Let $L/K, L'/K$ be two distinct cyclic extensions of prime degree p inside K^s. Then there exist infinitely many $v \in V_{K,f}$ which are split in L and non-split in L'.*

Proof. Clearly L and L' are linearly disjoint over K. Let M be the compositum LL'. Since M/L is non-trivial, there are infinitely many places w of L which are non-split in M. We can also require that w is over a place v which is unramified in M. Then since $e(M/w) = 1$ and $g(M/w) < p$, we have $f(M/w) = p$ and $g(M/w) = 1$. Thus there is a unique place u of M over w. Since M_u/K_v is unramified, $\mathrm{Gal}(M_u/K_v)$ is cyclic. But it is a subgroup of $\mathrm{Gal}(M/K) \cong \mathbb{Z}/p \times \mathbb{Z}/p$, so we must have $[M_u : K_v] = p$. Since $f(u/w) = p$, it follows that $L_w = K_v$, i.e., v splits in L. Such v must be non-split in L', as otherwise it would be split in M contradicting with $f(u/w) = p$. □

Remark 2.5.22. Let L/K be a finite Galois extension of global fields. Are there always infinitely many places of K which are split in L? Last semester we showed this for number fields, by showing that the set S of such places of K (excluding the archimedean places) has Dirichlet density

$$\lim_{s\to 1^+} \frac{\sum_{v\in S} |k_v|^{-s}}{\log \frac{1}{s-1}} = [L : K]^{-1}.$$

That argument involved three key ingredients:

(1) The Dedekind zeta function of any number field has meromorphic continuation to $\Re s > \sigma_0$ for some $\sigma_0 < 1$, and it has a simple pole at $s = 1$.
(2) For $s > 1/2$, we have $\sum_{v\in V_{K,f}} \sum_{m\geq 2} m^{-1}|k_v|^{-ms} < \infty$, and similarly for L in place of K.
(3) For $s > 1/2$, we have $\sum_{w\in V_{L,f}, f(w/K)>1} |l_w|^{-s} < \infty$, where l_w is the residue field of w.

All the above ingredients actually generalize to function fields L/K. For (1), the Dedekind zeta function of K is still defined as $\zeta_K(s) = \prod_{v\in V_K}(1 - |k_v|^{-s})^{-1}$, and it converges absolutely for $\Re s > 1$ and has a meromorphic continuation to $\mathbb{C}$ with the only poles being simple poles at 0 and 1. In fact, $\zeta_K(s)$ is the zeta function considered by Weil attached to the smooth projective geometrically connected curve X/k for which $K = k(X)$. Weil showed that

$$\zeta_K(s) = \frac{P(|k|^{-s})}{(1 - |k|^{-s})(1 - |k|^{1-s})},$$

where P is an integer coefficient polynomial of even degree. (Moreover, all complex roots of P have absolute value $|k|^{-1/2}$, so all zeros of $\zeta_K(s)$ satisfy $\Re s = 1/2$. The generalization of this to the zeta functions of higher dimensional algebraic varieties over a finite field is the famous "Riemann Hypothesis" among the Weil Conjectures, which was proved by Deligne.) To show (2), we use the following bound as in the number field case: For any $q \geq 2$,

$$\sum_{m\geq 2} \frac{1}{m} q^{-ms} \leq \sum_{m\geq 2} q^{-ms} = \frac{q^{-2s}}{1-q^{-s}} \leq \frac{q^{-2s}}{1-2^{-s}} \leq C \cdot q^{-2s},$$

where the constant C depends only on s, not on q. Then we use that K is a finite separable extension of $k(t)$, which implies that the number of $v \in V_K$ satisfying $[k_v : k] = n$ is less than a constant plus a positive constant times the number of monic irreducible polynomials over k of degree $\leq n$. The last number is $\leq |k|^n$ since every such polynomial is the minimal polynomial of an element of the degree n extension of k. Hence for $s > 1/2$ we have

$$\sum_v \sum_{m\geq 2} \frac{1}{m} |k_v|^{-ms} \leq C_1 \sum_{n\geq 1} |k|^n \sum_{m\geq 2} \frac{1}{m} |k|^{-nms} \leq C_2 \sum_{n\geq 1} (|k|^{1-2s})^n < +\infty.$$

To show (3), again using the above estimate for the number of $v \in V_K$ with $[k_v : k_n] = n$, we have

$$\sum_{w\in V_L, f(w/K)>1} |l_w|^{-s} \leq C_1 \sum_{v\in V_K} |k_v|^{-2s} \leq C_2 \sum_{n\geq 1} |k|^n |k|^{n(-2s)} = C_2 \sum_{n\geq 1} (|k|^{1-2s})^n < +\infty.$$

With all the three ingredients available, the rest of the argument is the same as in the number field case, yielding that the set S of places of K which are split in L has Dirichlet density $\lim_{s\to 1^+} \left(\sum_{v\in S} |k_v|^{-s}\right) / \log \frac{1}{s-1} = [L : K]^{-1}$.

We now prove the remaining case of the Second Inequality.

Proof of Theorem 2.4.2 for characteristic p. Let H be the image of $\mathrm{N}_{L/K} C_L$ under $\Phi : C_K/C_K^p \xrightarrow{\sim} \mathrm{Gal}(M/K)$. It suffices to prove $[\mathrm{Gal}(M/K) : H] = [M^H : K] \leq p$, and for this it suffices to prove that $M^H \subset L$. Now M^H is an Artin–Schreier extension of K, so it is the compositum of some degree p cyclic extensions of K (of the form $K(y)$ with $\wp(y) \in K$). It suffices to show that for any degree p cyclic extension L' of K in M which is different from L, we have $L' \not\subset M^H$. Write $L' = K(y)$, with $x = \wp(y) \in K$. We need to find $a \in \mathrm{N}_{L/K} \mathbb{A}_L^\times \subset \mathbb{A}_K^\times$ such that $\Phi(a)y \neq y$, or equivalently $\phi(x, a) \neq 0$. By Lemma 2.5.21, there exists a finite place v of K which is split in L, non-split in L', and such that $x \in \mathcal{O}_{K_v}$. Let $a \in \mathbb{A}_K^\times$ be the element whose coordinate at every $w \neq v$ is 1 and whose coordinate at v is a uniformizer $\pi_v \in K_v^\times$. Since v splits in L, we have $a \in \mathrm{N}_{L/K} \mathbb{A}_L^\times$. It remains to check that $\phi(x, a) \neq 0$. If not, then by Lemma 2.5.15 (1) we have $x \in \wp(K_v)$, which contradicts with the condition that v is non-split in L'. □

2.6. **Analytic proof of the Second Inequality.** There is a short analytic proof of the Second Inequality (Theorem 2.4.2), at least for number fields, based on the elementary properties of Weber L-functions established last semester. We explain the proof for number fields below, and leave the reader to consider whether the proof can be generalized to function fields. In this proof, the assumption that L/K has prime degree is irrelevant; it can be an arbitrary finite Galois extension.

Recall that a *modulus* of K is a formal product $\mathfrak{m} = \prod_{v\in V_K} v^{e_v}$, where e_v are non-negative integers almost all of which are zero, and for v real (resp. complex) e_v is only allowed to be

0 or 1 (resp. only allowed to be 0). We have the open subgroup

$$U_{\mathfrak{m}} = \prod_{v|\infty, v\nmid\mathfrak{m}} K_v^\times \times \prod_{v|\infty, v|\mathfrak{m}} K_{v,>0} \times \prod_{v\nmid\infty, v\nmid\mathfrak{m}} \mathcal{O}_{K_v}^\times \times \prod_{v\nmid\infty, v|\mathfrak{m}} (1+\mathfrak{m}_{K_v}^{e_v})$$

of $\mathbb{A}_K^\times$, and moreover every open subgroup of $\mathbb{A}_K^\times$ contains a $U_{\mathfrak{m}}$ for some $\mathfrak{m}$. The *ray class group* of modulus $\mathfrak{m}$ is defined as

$$\mathrm{Cl}_{\mathfrak{m}}(K) = \mathbb{A}_K^\times/(K^\times U_{\mathfrak{m}}) = C_K/\bar{U}_{\mathfrak{m}},$$

where $\bar{U}_{\mathfrak{m}}$ denotes the image of $U_{\mathfrak{m}}$ in C_K. This has the ideal theoretic interpretation as the quotient group of the group of fractional ideals coprime to $\mathfrak{m}$ modulo the principal fractional ideals generated by $x \in K^\times$ satisfying:

$$\begin{cases} x \in K_{v,>0}, & \forall v|\infty, v|\mathfrak{m}; \\ x \in 1+\mathfrak{m}_{K_v}^{e_v}, & \forall v\nmid\infty, v|\mathfrak{m} \end{cases}$$

where e_v is the exponent of v in $\mathfrak{m}$. Recall that $\mathrm{Cl}_{\mathfrak{m}}(K)$ is finite since it is both discrete (because $U_{\mathfrak{m}}$ is open) and compact (because C_K^1 is compact, and the idele norm restricted to $U_{\mathfrak{m}}$ is still surjective onto $\mathbb{R}_{>0}$).

For every character $\chi : \mathrm{Cl}_{\mathfrak{m}}(K) \to \mathbb{C}^\times$, the Weber L-function is defined as

$$L(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{m}} (1-\chi(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{-s})^{-1},$$

where $\mathfrak{p}$ runs over prime ideals of $\mathcal{O}_K$ coprime to $\mathfrak{m}$, and $\mathrm{N}(\mathfrak{p})$ is the size of the residue field. Last semester we showed that $L(s,\chi)$ has meromorphic continuation to $\Re s > \sigma_0$ for some $\sigma_0 < 1$, and it is holomorphic at $s=1$ for non-trivial χ and has a simple pole at $s=1$ for the trivial χ. (Assuming class field theory, we furthermore showed that $L(1,\chi) \neq 0$ for non-trivial χ, which is the key ingredient in the proof of the Chebotarev density theorem. In the following we will not use this, so the proof is not circular.)

Analytic proof of Theorem 2.4.2 for number fields. By local class field theory we know that $\mathrm{N}_{L/K}A_L^\times$ is an open subgroup of $\mathbb{A}_K^\times$, so we can find a modulus $\mathfrak{m}$ of K such that $U_{\mathfrak{m}} \subset \mathrm{N}_{L/K}A_L^\times$. Let H be the subgroup of $\mathrm{Cl}_{\mathfrak{m}}(K)$ generated by the prime ideals coprime to $\mathfrak{m}$ which are split in L. Every such prime ideal is an ideal norm from L, from which it easily follows that the image of $\mathrm{N}_{L/K}C_L$ in $\mathrm{Cl}_{\mathfrak{m}}(K) = C_K/\bar{U}_{\mathfrak{m}}$ contains H, and hence $[C_K : \mathrm{N}_{L/K}C_L] \leq [\mathrm{Cl}_{\mathfrak{m}}(K) : H]$. Write n for $[\mathrm{Cl}_{\mathfrak{m}}(K) : H]$. In the following we show that $n \leq [L:K]$.

For two real functions $f(s), g(s)$ defined on $(1, 1+\epsilon)$ for some $\epsilon > 0$, we write $f(s) \sim g(s)$ if $|f(s) - g(s)|$ is bounded as $s \to 1^+$. For every character $\chi : \mathrm{Cl}_{\mathfrak{m}}(K) \to \mathbb{C}^\times$, recall from last semester that

$$\log L(s,\chi) \sim \sum_{\mathfrak{p}\nmid\mathfrak{m}} \chi(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{-s}.$$

Taking the sum over all characters χ which are trivial on H, we obtain

$$\sum_{\chi:\mathrm{Cl}_{\mathfrak{m}}(K)/H\to\mathbb{C}^\times} \log L(s,\chi) \sim n \sum_{\mathfrak{p}\nmid\mathfrak{m}, \mathfrak{p}\in H} \mathrm{N}(\mathfrak{p})^{-s}.$$

For any non-trivial χ, we have either $\log L(s,\chi) \sim 0$ if $L(1,\chi) \neq 0$, or $\log L(s,\chi) \to -\infty$ as $s \to 1^+$ if $L(1,\chi) = 0$. For the trivial χ, we have $\log L(s,\chi) \sim \log \frac{1}{s-1}$ since $L(s,\chi)$ has a

simple pole at $s = 1$. Hence

$$\sum_{\chi:\mathrm{Cl}_{\mathfrak{m}}(K)/H\to\mathbb{C}^\times} \log L(s,\chi) = \log\frac{1}{s-1} + g(s)$$

where $g(s)$ is a function which is bounded *from the above* as $s \to 1^+$. We conclude that

$$\limsup_{s\to 1^+} \frac{\sum_{\mathfrak{p}\nmid\mathfrak{m},\mathfrak{p}\in H} \mathrm{N}(\mathfrak{p})^{-s}}{\log\frac{1}{s-1}} \le \frac{1}{n}.$$

On the other hand, the summation index set in the numerator contains the set S of primes which are coprime to $\mathfrak{m}$ and split in L. Last semester we showed that (cf. Remark 2.5.22)

$$\lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p})^{-s}}{\log\frac{1}{s-1}} = [L:K]^{-1}.$$

Hence $[L:K]^{-1} \le n^{-1}$, as desired. □

2.7. **Consequences for the Brauer group.** We have completed the proof of Theorem 2.4.1. Let L/K be a finite Galois extension of global fields, and write G for $\mathrm{Gal}(L/K)$. The vanishing of $\widehat{\mathbf{H}}^1(G, C_L)$ immediately implies the following result.

Theorem 2.7.1 (Brauer–Hasse-Noether Theorem)**.** *The natural map*

$$\widehat{\mathbf{H}}^2(G, L^\times) = \mathrm{Br}(L/K) \longrightarrow \widehat{\mathbf{H}}^2(G, \mathbb{A}_L^\times) \cong \bigoplus_v \mathrm{Br}(L_w/K_v)$$

is injective. □

Here for each place v of K we choose a place w of L above v, which will be tacitly done in the following. The above statement is classically known as the *Brauer–Hasse–Noether theorem*. In terms of central simple algebras, it states that a central simple algebra B over K is isomorphic to $M_n(K)$ if and only if the K_v-algebra $K_v \otimes_K B$ is isomorphic to $M_n(K_v)$ for all places v of K.

We use inv_v to denote the canonical injection $\mathrm{inv} : \mathrm{Br}(L_w/K_v) \hookrightarrow \mathbb{Q}/\mathbb{Z}$ as well as the composite map $\mathrm{Br}(L/K) \to \mathrm{Br}(L_w/K_v) \hookrightarrow \mathbb{Q}/\mathbb{Z}$. (For $L_w/K_v = \mathbb{C}/\mathbb{R}$, we define the invariant $\mathrm{Br}(L_w/K_v) \hookrightarrow \mathbb{Q}/\mathbb{Z}$ to be the unique isomorphism onto $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$, cf. Exercise 1.24.8.) Thus by the Brauer–Hasse–Noether theorem we have an injection

$$\oplus_v \mathrm{inv}_v : \mathrm{Br}(L/K) \hookrightarrow \bigoplus_v \mathbb{Q}/\mathbb{Z}.$$

Since each inv_v is compatible with inflation of local fields, it is easy to see that the above map is compatible with inflation $\mathrm{Br}(L/K) \hookrightarrow \mathrm{Br}(L'/K)$ for L'/K finite Galois containing L. Thus we obtain an injection

$$\oplus_v \mathrm{inv}_v : \mathrm{Br}(K) \hookrightarrow \bigoplus_v \mathbb{Q}/\mathbb{Z}.$$

Later we will see that the image consists precisely of $(t_v)_v$ satisfying $\sum_v t_v = 0$.

Corollary 2.7.2. *Let E/K be a finite separable extension. We denote places of E by w. We have a commutative diagram*

$$\begin{array}{ccc} \mathrm{Br}(K) & \xrightarrow{\oplus_v \mathrm{inv}_v} & \bigoplus_v \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow \\ \mathrm{Br}(E) & \xrightarrow{\oplus_w \mathrm{inv}_w} & \bigoplus_w \mathbb{Q}/\mathbb{Z} \end{array}$$

where the vertical map on the right sends $(t_v)_v$ to $(u_w)_w$ with $u_w = [E_w : K_v]t_v$ for $w|v$. In particular, an element $x \in \mathrm{Br}(K)$ lies in the kernel of $\mathrm{Res} : \mathrm{Br}(K) \to \mathrm{Br}(E)$ if and only if for every $v \in V_K$ and $w \in V_L$ above v we have $[E_w : K_v] \mathrm{inv}_v(x) = 0 \in \mathbb{Q}/\mathbb{Z}$.

Remark 2.7.3. If E/K is finite Galois, then the condition $[E_w : K_v] \mathrm{inv}_v(x) = 0$ depends only on v, not on w. In this case the kernel of $\mathrm{Res} : \mathrm{Br}(K) \to \mathrm{Br}(E)$ is $\mathrm{Br}(E/K) \subset \mathrm{Br}(K)$.

Proof. In view of the functoriality of the local invariant with respect to restriction (Proposition 1.22.2), it suffices to check that for each finite Galois extension L/K containing E the following diagram commutes:

$$\begin{array}{ccc} \widehat{\mathbf{H}}^2(\mathrm{Gal}(L/K), \mathbb{A}_L^\times) & \xrightarrow{\cong} & \bigoplus_v \mathrm{Br}(L_u/K_v) \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle (x_v)\mapsto(y_w), y_w = \mathrm{Res}\, x_v \text{ for } w|v} \\ \widehat{\mathbf{H}}^2(\mathrm{Gal}(L/E), \mathbb{A}_L^\times) & \xrightarrow{\cong} & \bigoplus_w \mathrm{Br}(L_{u'}/E_w) \end{array}$$

Here, for $w|v$, the chosen place u of L above v as in $\mathrm{Br}(L_u/K_v)$ may be different from the chosen place u' of L above w as in $\mathrm{Br}(L_{u'}/K_w)$ (as each place u of L can be only over one place w of E, to be sure), but we have a canonical isomorphism[7] $\mathrm{Br}(L_u/K_v) \cong \mathrm{Br}(L_{u'}/K_v)$ and we use this to define the restriction map $\mathrm{Res} : \mathrm{Br}(L_u/K_v) \to \mathrm{Br}(L_{u'}/E_w)$.

We claim that the projection $\widehat{\mathbf{H}}^2(\mathrm{Gal}(L/K), \mathbb{A}_L^\times) \cong \bigoplus_v \mathrm{Br}(L_u/K_v) \to \mathrm{Br}(L_u/K_v)$ is equal to the composition

$$\widehat{\mathbf{H}}^2(\mathrm{Gal}(L/K), \mathbb{A}_L^\times) \xrightarrow{\mathrm{Res}} \widehat{\mathbf{H}}^2(D(u/v), \mathbb{A}_L^\times) \xrightarrow{\mathrm{pr}_u} \widehat{\mathbf{H}}^2(D(u/v), L_u^\times) = \mathrm{Br}(L_u/K_v),$$

where the second map is induced by the projection $\mathrm{pr}_u : \mathbb{A}_L^\times \to L_u^\times$. Indeed, the claim follows easily from a fact about the Shapiro isomorphism in Exercise 2.7.4 below.

Note also that the composite map in the claim is independent of the choice of u (with respect to the canonical isomorphism $\mathrm{Br}(L_u/K_w) \cong \mathrm{Br}(L_{u'}/K_w)$), which again follows from applying the fundamental fact mentioned in the footnote to the $\mathrm{Gal}(L/K)$-module $\mathbb{A}_L^\times$. Thus by the claim (applied to both L/K and L/E) and by the transitivity property of restriction maps, the desired commutative diagram follows from the following obvious commutative diagram for $u|w|v$:

$$\begin{array}{ccc} \widehat{\mathbf{H}}^2(D(u/v), \mathbb{A}_L^\times) & \xrightarrow{\mathrm{pr}_u} & \widehat{\mathbf{H}}^2(D(u/v), L_u^\times) \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} \\ \widehat{\mathbf{H}}^2(D(u/w), \mathbb{A}_L^\times) & \xrightarrow{\mathrm{pr}_u} & \widehat{\mathbf{H}}^2(D(u/w), L_u^\times) \end{array}$$

[7] This results from the choice of any K_v-isomorphism $L_u \xrightarrow{\sim} L_{u'}$; the canonicity follows from the following fundamental fact which can be checked easily by dimension shifting: Let G be a finite group and X a G-module. For any $g \in G$, we have compatible isomorphisms $G \xrightarrow{\sim} G, h \mapsto ghg^{-1}$ and $X \xrightarrow{\sim} X, x \mapsto gx$, and so by transport of structure we obtain an automorphism of $\widehat{\mathbf{H}}^q(G, X)$. The fundamental fact is that this automorphism is the identity.

□

Exercise 2.7.4. Let G be a finite group and D a subgroup. Let X be a D-module. We identify X with the subgroup $[1] \otimes X$ of $\mathrm{Ind}_D^G X = \mathbb{Z}[G] \otimes_{\mathbb{Z}[D]} X$. Then as an abelian group we have a direct sum decomposition $\mathrm{Ind}_D^G X = \bigoplus_{g \in G/D} g \cdot X$. Let $\mathrm{pr} : \mathrm{Ind}_D^G X \to X$ be the projection to the direct factor indexed by 1. Show that pr is D-linear. Then show that the Shapiro isomorphism $\widehat{\mathbf{H}}^q(G, \mathrm{Ind}_D^G X) \cong \widehat{\mathbf{H}}^q(D, X)$ is equal to the composition

$$\widehat{\mathbf{H}}^q(G, \mathrm{Ind}_D^G X) \xrightarrow{\mathrm{Res}} \widehat{\mathbf{H}}^q(D, \mathrm{Ind}_D^G X) \xrightarrow{\mathrm{pr}} \widehat{\mathbf{H}}^q(D, X).$$

Exercise 2.7.5. Let G be a finite group, H and D subgroups. For each $i \in H\backslash G/D$, let $D_i = iDi^{-1} \cap H$, which is a subgroup of H well-defined up to conjugation by H. Let X be a D-module. For each i, let X_i be the D_i-module whose underlying group is X and the D_i-action is induced by $D_i \hookrightarrow D, g \mapsto i^{-1}gi$. Let $M = \mathrm{Ind}_D^G X$. Show that as H-module we have $M \cong \prod_{i \in H\backslash G/D} \mathrm{Ind}_{D_i}^H X_i$ ("Mackey's formula"), and we have a commutative diagram

$$\begin{array}{ccccc}
\widehat{\mathbf{H}}^q(G, M) & \xrightarrow{\mathrm{Res}} & \widehat{\mathbf{H}}^q(H, M) & \xrightarrow{\cong} & \prod_{i \in H\backslash G/D} \widehat{\mathbf{H}}^q(H, \mathrm{Ind}_{D_i}^H X_i) \\
\cong \downarrow \text{Shapiro} & & & & \cong \downarrow \prod_i \text{Shapiro} \\
\widehat{\mathbf{H}}^q(D, X) & & \xrightarrow{\prod_{i \in H\backslash G/D} \mathrm{Res}_i} & & \prod_{i \in H\backslash G/D} \widehat{\mathbf{H}}^q(D_i, X_i)
\end{array}$$

where Res_i denotes restriction along $D_i \hookrightarrow D, g \mapsto i^{-1}gi$.

The following is another consequence of the vanishing of $\widehat{\mathbf{H}}^1(G, C_L)$.

Theorem 2.7.6 (Hasse Norm Theorem)**.** *Let L/K be a finite cyclic extension of global fields. Then $x \in K^\times$ lies in $\mathrm{N}_{L/K} L^\times$ if and only if $x \in \mathrm{N}_{L_w/K_v} L_w^\times$ for all places v of K.*

Proof. Let $G = \mathrm{Gal}(L/K)$. Since G is cyclic, we have $\widehat{\mathbf{H}}^{-1}(G, C_L) \cong \widehat{\mathbf{H}}^1(G, C_L) = 0$. Hence the natural map

$$\widehat{\mathbf{H}}^0(G, L^\times) = K^\times/\mathrm{N}_{L/K} L^\times \longrightarrow \widehat{\mathbf{H}}^0(G, \mathbb{A}_L^\times) = \mathbb{A}_K^\times/\mathrm{N}_{L/K} \mathbb{A}_L^\times$$

is injective. To deduce the theorem, it remains to note that any $x \in K^\times$ automatically satisfies $x \in \mathrm{N}_{L_w/K_v} \mathcal{O}_{L_w}^\times$ for almost all v, due to the surjectivity of $\mathrm{N}_{L_w/K_v} : \mathcal{O}_{L_w}^\times \to \mathcal{O}_{K_v}^\times$ for unramified $w|v$. □

Example 2.7.7. Let L be a quadratic extension of K of the form $L = K(\sqrt{b})$ with $b \in K^\times - (K^\times)^2$. Then an element $a \in K^\times$ is a norm from L if and only if there are $x, y \in K$ such that $x^2 - by^2 = a$. Since b is not a square, this happens if and only if the equation $x^2 - by^2 - az^2 = 0$ has a *non-trivial* solution $x, y, z \in K$ (non-trivial in the sense that at least one of x, y, z is non-zero). Similarly, a is a norm from L_w if and only if the above equation has a non-trivial solution in K_v. Since every non-degenerate quadratic form in three variables $Q(x, y, z)$ over K can be diagonalized, we conclude that for any such Q, it has a non-trivial zero over K if and only if it has a non-trivial zero over K_v for all $v \in V_K$. Later we will generalize this statement to quadratic forms in an arbitrary number of variables, which is called the *Hasse principle*.

2.8. **Proof of the Reciprocity Law.** We had set out to verify the assumptions in Tate's theorem, namely that for any finite Galois extension L/K of global fields with $G = \mathrm{Gal}(L/K)$, we have $\widehat{\mathbf{H}}^1(G, C_L) = 0$ and $\widehat{\mathbf{H}}^2(G, C_L) \cong \mathbb{Z}/[L : K]$. We have already achieved the first but not yet the second. Once we know this, we can apply Tate's theorem and obtain an isomorphism $\widehat{\mathbf{H}}^q(G, \mathbb{Z}) \xrightarrow{\sim} \widehat{\mathbf{H}}^{q+2}(G, C_L)$ for all $q \in \mathbb{Z}$, and in particular for $q = -2$ obtain the global Artin map $C_K/\mathrm{N}_{L/K}C_L \xrightarrow{\sim} G^{\mathrm{ab}}$. However, these goals are in fact stronger than just proving the global Reciprocity Law (Theorem 2.1.1). In the following we take the slightly different point of view, namely that the global Artin map is already determined by the local Artin maps via local-global compatibility, and prove the reciprocity law directly, without establishing the structure of $\widehat{\mathbf{H}}^2(G, C_L)$. In the meantime, we prove several statements about the Brauer group, which we will later use to obtain a canonical isomorphism $\widehat{\mathbf{H}}^2(G, C_L) \cong \mathbb{Z}/[L : K]$ and thereby finishing the program of checking the assumptions in Tate's theorem. We will then also show that the global Artin map provided by Tate's theorem agrees with the one provided by local-global compatibility, completing the logical circle.

Observe that if the global Artin map exists as in the global reciprocity law and if the local-global compatibility holds, then for every finite abelian extension L/K the composite map

$$\mathbb{A}_K^\times \to C_K \xrightarrow{\psi_{L/K}} \mathrm{Gal}(L/K)$$

must be given by the formula

$$(a_v) \longmapsto \prod_v \psi_{L_w/K_v}(a_v).$$

Here ψ_{L_w/K_v} is the local Artin map $K_v^\times \to \mathrm{Gal}(L_w/K_v)$, and as usual we embed $\mathrm{Gal}(L_w/K_v)$ canonically into $\mathrm{Gal}(L/K)$. Note that the product is finite, since ψ_{L_w/K_v} kills $\mathcal{O}_{K_v}^\times$ whenever L_w/K_v is unramified.

Since we already have the local Artin maps, we can actually use the above formula to *define* the global Artin map $\psi = \psi_{L/K} : \mathbb{A}_K^\times \to \mathrm{Gal}(L/K)$. This is clearly a continuous homomorphism. However, the condition that ψ factors through the quotient C_K is non-trivial to prove. We shall refer to this condition as the *Artin reciprocity law*, and prove it in the sequel.

Before proving the Artin reciprocity law, we first note that it essentially implies the entire Reciprocity Law (Theorem 2.1.1).

Lemma 2.8.1. *Suppose $\psi_{L/K}$ factors through C_K. Then the induced map $C_K \to \mathrm{Gal}(L/K)$ is surjective with kernel $\mathrm{N}_{L/K}C_L$.*

Proof. Surjectivity immediately follows from Corollary 2.3.6 (2) and the fact that for L_w/K_v unramified ψ_{L_w/K_v} sends a uniformizer to the Frobenius. Since ψ_{L_w/K_v} has kernel $\mathrm{N}_{L_w/K_v}L_w^\times$, the kernel of $\psi_{L/K} : C_K \to \mathrm{Gal}(L/K)$ clearly contains $\mathrm{N}_{L/K}C_L$. Hence $\psi_{L/K}$ induces a surjection $C_K/\mathrm{N}_{L/K}C_L \to \mathrm{Gal}(L/K)$. By the Second Inequality (Theorem 2.4.1 (2)), the size of the left hand side is not greater than the right hand side. Hence the kernel of $\psi_{L/K} : C_K \to \mathrm{Gal}(L/K)$ must be $\mathrm{N}_{L/K}C_L$. □

We shall prove the Artin reciprocity law together with another statement about the Brauer group. We label the two statements:

(A) (Artin reciprocity law.) For every finite abelian extension L/K, the map $\psi_{L/K} : \mathbb{A}_K^\times \to \mathrm{Gal}(L/K)$ defined by taking the product of the local Artin maps factors through C_K.

(B) Every element $x \in \mathrm{Br}(K)$ satisfies $\sum_v \mathrm{inv}_v(x) = 0 \in \mathbb{Q}/\mathbb{Z}$.

Lemma 2.8.2. *For every finite abelian extension L/K, statement (B) for all elements $x \in \mathrm{Br}(L/K) \subset \mathrm{Br}(L)$ implies statement (A) for L/K. If L/K is cyclic, then the converse holds.*

Proof. Let L/K be a finite abelian extension. Write G for $\mathrm{Gal}(L/K)$ and G_v for $\mathrm{Gal}(L_w/K_v) \subset G$. Write ψ for $\psi_K : \mathbb{A}_K^\times \to G$, and write ψ_v for $\Psi_{L_w/K_v} : K_v^\times \to G_v$. Recall from Lemma 1.24.3 that ψ_v has the following characterization: For every $\chi \in \widehat{\mathbf{H}}^1(G_v, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G_v, \mathbb{Q}/\mathbb{Z})$ and every $a_v \in K_v^\times$, we have

$$\chi(\psi_v(a_v)) = \mathrm{inv}_v(\bar{a}_v \cup \delta\chi) \in \mathbb{Q}/\mathbb{Z}.$$

Here $\bar{a}_v$ denotes the image of a_v in $K_v^\times/\mathrm{N}_{L_w/K_v} L_w^\times = \widehat{\mathbf{H}}^0(G_v, L_w^\times)$, and $\delta : \widehat{\mathbf{H}}^1(G_v, \mathbb{Q}/\mathbb{Z}) \to \widehat{\mathbf{H}}^2(G_v, \mathbb{Z})$ is attached to the short exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$.

As we claimed in the proof of Corollary 2.7.2, the projection to the v-th component $\widehat{\mathbf{H}}^2(G, \mathbb{A}_L^\times) \cong \bigoplus_v \mathrm{Br}(L_w/K_v) \to \mathrm{Br}(L_w/K_v)$ is equal to the composite map

$$\widehat{\mathbf{H}}^2(G, \mathbb{A}_L^\times) \xrightarrow{\mathrm{Res}} \widehat{\mathbf{H}}^2(G_v, \mathbb{A}_L^\times) \to \widehat{\mathbf{H}}^2(G_v, L_w^\times).$$

Also, the restriction map $\widehat{\mathbf{H}}^1(G, \mathbb{Q}/\mathbb{Z}) \to \widehat{\mathbf{H}}^1(G_v, \mathbb{Q}/\mathbb{Z})$ as in group cohomology is just the usual restriction map $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(G_v, \mathbb{Q}/\mathbb{Z})$. Hence using the compatibility of cup product with restriction we compute: for $a = (a_v)_v \in \mathbb{A}_K^\times$ and $\chi \in \widehat{\mathbf{H}}^1(G, \mathbb{Q}/\mathbb{Z})$,

$$\chi(\psi(a)) = \sum_v \chi|_{G_v}(\psi_v(a_v)) = \sum_v \mathrm{inv}_v(\bar{a}_v \cup \delta\chi|_{G_v}) = \sum_v \mathrm{inv}_v(\bar{a} \cup \delta\chi),$$

where $\bar{a} \in \widehat{\mathbf{H}}^0(G, \mathbb{A}_L^\times), \delta\chi \in \widehat{\mathbf{H}}^2(G, \mathbb{Q}/\mathbb{Z})$, and so $\bar{a} \cup \delta\chi \in \widehat{\mathbf{H}}^2(G, \mathbb{A}_L^\times)$ and we write inv_v for the composition of the projection of $\widehat{\mathbf{H}}^2(G, \mathbb{A}_L^\times)$ to $\mathrm{Br}(L_w/K_v)$ followed by the local invariant map $\mathrm{Br}(L_w/K_v) \hookrightarrow \mathbb{Q}/\mathbb{Z}$. This formula for $\chi(\psi(a))$ gives a characterization of ψ.

If (B) holds for all elements of $\mathrm{Br}(L/K)$, then for $a \in K^\times \subset \mathbb{A}_K^\times$ we obtain $\chi(\psi(a)) = 0$ for all χ. It follows that $\psi(a) = 1$, so (A) holds.

Conversely, assume that L/K is finite cyclic and that (A) holds for L/K. In order to show (B) for all elements of $\mathrm{Br}(L/K)$, it suffices to show that all such elements can be written as $\bar{a} \cup \delta\chi$ for some $a \in K^\times$ and $\chi \in \widehat{\mathbf{H}}^1(G, \mathbb{Q}/\mathbb{Z})$ (since by (A) we have $\chi(\psi(a)) = 0$). Since $\widehat{\mathbf{H}}^2(G, \mathbb{Q})$ is killed by $|G|$ and $|G|$ is invertible in $\mathbb{Q}$, we have $\widehat{\mathbf{H}}^2(G, \mathbb{Q}) = 0$. Hence $\widehat{\mathbf{H}}^1(G, \mathbb{Q}/\mathbb{Z})$ surjects onto $\widehat{\mathbf{H}}^2(G, \mathbb{Z})$. Recall that the latter is a cyclic group of order $|G|$ in the current case of a cylic group G. Fix $\chi \in \widehat{\mathbf{H}}^1(G, \mathbb{Q}/\mathbb{Z})$ such that $\delta\chi$ is a generator of $\widehat{\mathbf{H}}^2(G, \mathbb{Z})$. Recall that for every $q \in \mathbb{Z}$ and every G-module M, $\cdot \cup \delta\chi$ is an isomorphism $\widehat{\mathbf{H}}^q(G, M) \xrightarrow{\sim} \widehat{\mathbf{H}}^{q+2}(G, M)$. This shows that every element of $\mathrm{Br}(L/K)$ can be written in the desired form. □

Lemma 2.8.3. *We call an extension L/K* good *if it is a finite cyclic extension contained in a cyclotomic extension of K in the number field case, or if it is of the form $k_n \otimes_k K$ in the function field case, where k denotes the constant field of K and k_n denotes the degree n extension of k. (In the latter case the extension is also cyclic.) We have*

$$\mathrm{Br}(K) = \bigcup_{L/K \ \mathit{good}} \mathrm{Br}(L/K).$$

Proof. By Corollary 2.7.2, it suffices to show that for every finite subset S of $V_{K,f}$ and $m \in \mathbb{Z}_{\geq 1}$, there exists a good extension L/K such that it is totally complex (i.e., every

archimedean place of L is complex) and such that local degrees $[L_w : K_v]$ of L over $v \in S$ are all divisible by m.

In the function field case, for any $v \in V_K$ such that $k_v \subset k_n$, there is a unique place of $k_n \otimes_k K$ above v and the local extension is unramified of degree $[k_n : k_v]$. Hence it suffices to take $n = m \prod_{v \in S} [k_v : k]$.

In the number field case, if we can already do this for $K = \mathbb{Q}$, then for general (K, S, m), we find a good extension $M/\mathbb{Q}$ which is totally complex and whose local degree over every prime p of $\mathbb{Q}$ below S is divisible by $m \cdot [K : \mathbb{Q}]!$. Let $L = MK$. This is a totally complex good extension of K. For every $w \in V_L$ dividing $v \in S$ and $u \in V_M$, we have $[L_w : K_v] = [L_w : \mathbb{Q}_p]/[K_v : \mathbb{Q}_p]$, and this is divisible by m since the numerator is divisible by $[M_u : \mathbb{Q}_p]$ and the denominator is a divisor of $[K : \mathbb{Q}]!$.

Thus we have reduced to the case $K = \mathbb{Q}$. We claim that for every prime number q and integer $f \geq 1$, there exists a good extension $L(q)'/\mathbb{Q}$ whose degree is a power of q and whose local degree at every $p \in S$ is $q^{f(p)}$ for some $f(p) \geq f$. Moreover, if $q = 2$, then $L(q)'$ can be taken to be totally complex.

One we know the claim, we may assume that $2|m$ and write $m = \prod_{i=1}^{t} q_i^{f_i}$ where the q_i's are distinct primes. Then for each i we find a good extension $L(q_i)'/\mathbb{Q}$ as above whose degree is a power of q_i and whose local degree at every $p \in S$ is $q_i^{f(p)}$ for some $f(p) \geq f_i$. Let $L = L(q_1)' \cdots L(q_t)'$. Then $L/\mathbb{Q}$ satisfies the desired conditions.

It remains to prove the claim. First assume q is an odd prime. Let $r \geq 2$ be a large integer. Let $L(q) = \mathbb{Q}(\zeta_{q^r})$. Then $\mathrm{Gal}(L(q)/\mathbb{Q}) \cong (\mathbb{Z}/q^r\mathbb{Z})^\times$. This is a cyclic group of order $(q-1)q^{r-1}$, and so it decomposes into the direct product of two cyclic groups $C_{q-1} \times C_{q^{r-1}}$. Let $L(q)' = L(q)^{C_{q-1}}$. This is a good extension of $\mathbb{Q}$ of degree q^{r-1}. For every prime p, the local degree of $L(q)'$ at p is the local degree of $L(q)$ at p divided by a number which is a divisor of $[L(q) : L(q)'] = q - 1$. Note that the local degree of $L(q)$ at p tends to infinity as $r \to +\infty$. (To see this, either use the fact that this number is $(q-1)q^{r-1}$ when $q = p$ (in which case p is totally ramified) and is the order of p in $(\mathbb{Z}/q^r\mathbb{Z})^\times$ when $q \neq p$ (in which case p is unramified), or use the fact that every finite extension of $\mathbb{Q}_p$ contains only finitely many roots of unity, say by using the exponential map.) It follows that the local degree of $L(q)'$ at p tends to infinity as $r \to +\infty$. The claim is proved in this case.

Now consider $q = 2$. Again let r be large and let $L(2) = \mathbb{Q}(\zeta_{2^r})$. Then $\mathrm{Gal}(L(2)/\mathbb{Q}) = (\mathbb{Z}/2^r\mathbb{Z})^\times$, and this has a direct product decomposition $\{\pm 1\} \times H$, where $H = \{x \in (\mathbb{Z}/2^r\mathbb{Z})^\times \mid x \equiv 1 \mod 4\}$ and H is cyclic of order 2^{r-2}. (To see that H is cyclic, one can for instance use the isomorphism $\exp : 4\mathbb{Z}_2 \xrightarrow{\sim} 1 + 4\mathbb{Z}_2$, and consider $\gamma = \exp(4)$. We have $\exp(2^k\mathbb{Z}_2) = 1 + 2^k\mathbb{Z}_2$ for all $k \geq 2$, so $(\gamma \mod 2^r)$ is a generator of H.) Let $L(2)' = \mathbb{Q}(\zeta_{2^r} - \zeta_{2^r}^{-1})$. By the exercise below, $\mathrm{Gal}(L(2)'/\mathbb{Q}) \cong H$, so this is a good extension of $\mathbb{Q}$ of degree 2^{r-2}, and by the same argument as in the odd case, for each prime p the local degree of $L(2)'$ over p tends to infinity as $r \to +\infty$. Note that $L(2)'$ is totally complex. The claim is proved. □

Exercise 2.8.4. The natural map $\mathrm{Gal}(L(2)/\mathbb{Q}) \to \mathrm{Gal}(L(2)'/\mathbb{Q})$ induces an isomorphism $H \xrightarrow{\sim} \mathrm{Gal}(L(2)'/\mathbb{Q})$.

Theorem 2.8.5. *Both statements (A) and (B) hold.*

Proof. By Lemmas 2.8.2 and 2.8.3, we only need to prove statement (A) for a good extension L/K. In the function field case, if $L = k_n \otimes_k K$, then $\mathrm{Gal}(L/K)$ is cyclic of order n generated by Frob_k, the Frobenius generator of $\mathrm{Gal}(k_n/k)$. The extension L/K is unramified everywhere, and moreover for every $v \in V_K$ the Frobenius $\mathrm{Frob}_v \in \mathrm{Gal}(L/K)$ is equal to

$\mathrm{Frob}_k^{[k_v:k]}$. Hence for $a \in K^\times$, we have

$$\psi_{L/K}(a) = \prod_v \mathrm{Frob}_v^{\mathrm{ord}_v(a)} = \mathrm{Frob}_k^{\sum_v \mathrm{ord}_v(a)[k_v:k]},$$

and this is 1 since

$$1 = \prod_v \|a\|_v = \prod_v |k|^{-[k_v:k]\,\mathrm{ord}_v(a)}.$$

Consider the number field case. For any finite Galois extension L'/K containing L/K, we have a commutative diagram

$$\begin{array}{ccc} & & \mathrm{Gal}(L'/K) \\ & \overset{\psi_{L'/K}}{\nearrow} & \downarrow \\ \mathbb{A}_K^\times & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

which follows from the similar functoriality property of each local Artin map. Hence we may replace L/K by a cyclotomic extension $K(\zeta_n)/K$. Now we also have a commutative diagram

$$\begin{array}{ccc} \mathbb{A}_K^\times & \xrightarrow{\psi_{K(\zeta_n)/K}} & \mathrm{Gal}(K(\zeta_n)/K) \\ \downarrow{\scriptstyle \mathrm{N}_{K/\mathbb{Q}}} & & \downarrow \\ \mathbb{A}_\mathbb{Q}^\times & \xrightarrow{\psi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}} & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \end{array}$$

which follows from the norm functoriality of local Artin maps. Since $\mathrm{N}_{K/\mathbb{Q}}$ maps $K^\times \subset \mathbb{A}_K^\times$ into $\mathbb{Q}^\times \subset \mathbb{A}_\mathbb{Q}^\times$, we reduce to the case where $K = \mathbb{Q}$. It remains to prove that $\psi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}$ kills $\mathbb{Q}^\times \subset \mathbb{A}_\mathbb{Q}^\times$.

We have the canonical isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, where $\mu \in (\mathbb{Z}/n\mathbb{Z})^\times$ corresponds to the automorphism $\zeta_n \mapsto \zeta_n^\mu$. Since the local Artin map agrees with the explicit map given by Lubin–Tate theory, we know that for every prime p the local Artin map $\psi_p : \mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) \subset (\mathbb{Z}/n\mathbb{Z})^\times$ has the following description: Write $n = p^a b$ with $p \nmid b$, and we have $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p^a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$. For an arbitrary element $x = p^t u \in \mathbb{Q}_p^\times$ with $t \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$, we have

$$\psi_p(x) = (u^{-1} \mod p^a, \quad p^t \mod b) \in (\mathbb{Z}/p^a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times.$$

Also ψ_∞ is the sign map $\mathbb{R}^\times \to \{\pm 1\} \subset (\mathbb{Z}/n\mathbb{Z})^\times$. Using this, it is straightforward to check that for every prime number l we have

$$\prod_{v \in V_\mathbb{Q}} \psi_v(l) = \prod_p \psi_p(l) = 1 \in (\mathbb{Z}/n\mathbb{Z})^\times,$$

finishing the proof. □

At this point we have obtained the global Artin map $\psi_{L/K} : C_K \to \mathrm{Gal}(L/K)$ for every finite abelian extension L/K, which we know satisfies local-global compatibility (by design), and induces an isomorphism $C_K/\mathrm{N}_{L/K}C_L \xrightarrow{\sim} \mathrm{Gal}(L/K)$ (by Lemma 2.8.1). It is compatible when we enlarge L since the local Artin map satisfies the similar property (which we already used in the proof of Theorem 2.8.5 above), and so we obtain the desired global Artin map $\psi_K : C_K \to G_K^{\mathrm{ab}}$, completing the proof of the global Reciprocity Law (Theorem 2.1.1) as well as local-global compatibility (Theorem 2.1.6).

2.9. **The second cohomology of the idele class group.** Our goal is to show that there is a canonical isomorphism

$$\mathrm{inv} : \widehat{\mathbf{H}}^2(\mathrm{Gal}(L/K), C_L) \xrightarrow{\sim} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

for every finite Galois extension L/K, thus finishing checking the assumptions in Tate's theorem.

To simplify notation, we write $\mathrm{Br}_A(L/K)$ for $\widehat{\mathbf{H}}^2(\mathrm{Gal}(L/K), \mathbb{A}_L^\times)$, and write $\mathrm{Br}_C(L/K)$ for $\widehat{\mathbf{H}}^2(\mathrm{Gal}(L/K), C_L)$. We already saw that $\mathrm{Br}_A(L/K)$ is the direct sum of the local Brauer groups. The main object of study is $\mathrm{Br}_C(L/K)$.

Since $\widehat{\mathbf{H}}^1(\mathrm{Gal}(L/K), \mathbb{A}_L^\times) = \bigoplus_v \widehat{\mathbf{H}}^1(\mathrm{Gal}(L_w/K_v), L_w^\times) = 0$, the inflation map $\mathrm{Br}_A(L/K) \to \mathrm{Br}_A(L'/K)$ is injective for every pair of finite Galois extensions $L/K, L'/K$ with $L \subset L'$. Similarly, since $\widehat{\mathbf{H}}^1(\mathrm{Gal}(L/K), C_L) = 0$, the inflation map $\mathrm{Br}_C(L/K) \to \mathrm{Br}_C(L'/K)$ is injective. We thus define the "absolute versions"

$$\mathrm{Br}_A(K) := \varinjlim_{L/K} \mathrm{Br}_A(L/K) = \bigcup_{L/K} \mathrm{Br}_A(L/K),$$
$$\mathrm{Br}_C(K) := \varinjlim_{L/K} \mathrm{Br}_C(L/K) = \bigcup_{L/K} \mathrm{Br}_C(L/K).$$

By the exact sequence $1 \to L^\times \to \mathbb{A}_L^\times \to C_L \to 1$ and the vanishing of $\widehat{\mathbf{H}}^1(\mathrm{Gal}(L/K), C_L)$, we have exact sequences

$$0 \to \mathrm{Br}(L/K) \to \mathrm{Br}_A(L/K) \to \mathrm{Br}_C(L/K),$$
$$0 \to \mathrm{Br}(K) \to \mathrm{Br}_A(K) \to \mathrm{Br}_C(K).$$

The map $\mathrm{Br}_A(L/K) \to \mathrm{Br}_C(L/K)$ is not always surjective, but we will show that $\mathrm{Br}_A(K) \to \mathrm{Br}_C(K)$ is surjective.

We set

$$R := \bigoplus_{v \in V_{K,\mathrm{real}}} \frac{1}{2}\mathbb{Z}/\mathbb{Z} \oplus \bigoplus_{v \in V_{K,f}} \mathbb{Q}/\mathbb{Z}.$$

On $\mathrm{Br}_A(L/K) \cong \bigoplus_{v \in V_K} \mathrm{Br}(L_w/K_v)$ we have the local invariants, and altogether they give an injective map

$$\bigoplus_v \mathrm{inv}_v : \mathrm{Br}_A(L/K) \hookrightarrow R,$$

whose image is $\bigoplus_v \frac{1}{[L_w:K_v]}\mathbb{Z}/\mathbb{Z}$. This is compatible with inflation, so we obtain an injective map

$$\bigoplus_v \mathrm{inv}_v : \mathrm{Br}_A(K) \hookrightarrow R.$$

We claim that it is also surjective. Indeed, for any finite subset $S \subset V_{K,f}$ and any $m \geq 1$, we showed in the proof of Lemma 2.8.3 that there exists a totally complex finite Galois extension L/K whose local degrees over S are all divisible by m. For such L, the image $\bigoplus_v \frac{1}{[L_w:K_v]}\mathbb{Z}/\mathbb{Z}$ of $\mathrm{Br}_A(L/K) \subset \mathrm{Br}_A(K)$ under $\bigoplus_v \mathrm{inv}_v$ contains $R_{S,m} := \bigoplus_{v \in V_{K,\mathrm{real}}} \frac{1}{2}\mathbb{Z}/\mathbb{Z} \oplus \bigoplus_{v \in S} \frac{1}{m}\mathbb{Z}/\mathbb{Z}$. But R is generated by $R_{S,m}$ for all choices of S and m. The desired surjectivity follows.

Let inv denote the composition

$$\mathrm{Br}_A(K) \xrightarrow[\cong]{\oplus_v \mathrm{inv}_v} R \xrightarrow{\sum_v} \mathbb{Q}/\mathbb{Z}.$$

By statement (B) in Theorem 2.8.5, we have inv $= 0$ on the image of $\mathrm{Br}(K) \to \mathrm{Br}_A(K)$. Therefore, denoting by $\mathrm{Br}_C(K)_{\mathrm{reg}}$ the image of $\mathrm{Br}_A(K) \to \mathrm{Br}_C(K)$, we have a canonical map $\mathrm{inv} : \mathrm{Br}_C(K)_{\mathrm{reg}} \to \mathbb{Q}/\mathbb{Z}$.

By Lemma 2.8.3, we have $\mathrm{Br}(K) = \bigcup_{L/K \text{ good}} \mathrm{Br}(L/K)$. Since the proof is by arguing that there exists a good extension L/K killing all local invariants of an element, the same proof also yields that $\mathrm{Br}_A(K) = \bigcup_{L/K \text{ good}} \mathrm{Br}_A(L/K)$.

Proposition 2.9.1. *The map* $\mathrm{inv} : \mathrm{Br}_C(K)_{\mathrm{reg}} \to \mathbb{Q}/\mathbb{Z}$ *is an isomorphism.*

Proof. Surjectivity follows from the surjectivity of $\bigoplus_v \mathrm{inv}_v : \mathrm{Br}_A(K) \xrightarrow{\sim} R$ and the obvious surjectivity of $\sum : R \to \mathbb{Q}/\mathbb{Z}$.

For injectivity, let $x \in \mathrm{Br}_C(K)_{\mathrm{reg}}$ be such that $\mathrm{inv}(x) = 0$. There is a good extension L/K and an element $y \in \mathrm{Br}_A(L/K)$ mapping to x, and by the definition of inv on $\mathrm{Br}_C(K)_{\mathrm{reg}}$ we have $\mathrm{inv}(y) = 0$. Note that in general, the image of $\mathrm{inv} : \mathrm{Br}_A(L/K) \to \mathbb{Q}/\mathbb{Z}$ is always $\frac{1}{N}\mathbb{Z}/\mathbb{Z}$, where N is the least common multiple of all local degrees of L/K. For L/K a good extension (or just a cyclic extension), in view of Corollary 2.3.6 (2) we must have $N = [L : K]$. Hence in this case inv induces a surjection $\mathrm{Br}_A(L/K)/\mathrm{Br}(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$, implying that $[\mathrm{Br}_A(L/K) : \mathrm{Br}(L/K)] \geq [L : K]$. On the other hand we have an injection $\mathrm{Br}_A(L/K)/\mathrm{Br}(L/K) \to \mathrm{Br}_C(L/K)$, implying that $[\mathrm{Br}_A(L/K) : \mathrm{Br}(L/K)] \leq |\mathrm{Br}_C(L/K)|$, and this is $\leq [L : K]$ by the second inequality. We conclude that $\mathrm{Br}(L/K)$ is exactly the kernel of $\mathrm{inv} : \mathrm{Br}_A(L/K) \to \mathbb{Q}/\mathbb{Z}$, and so $y \in \mathrm{Br}(L/K)$. It then follows that $x = 0$, as desired. □

Corollary 2.9.2 (The "fundamental exact sequence of global class field theory")**.** *Let L/K be a finite Galois extension, and let N be the least common multiple of the local degrees $[L_w : K_v]$. Denote*

$$R := \bigoplus_{v \in V_{K,\mathrm{real}}} \frac{1}{2}\mathbb{Z}/\mathbb{Z} \oplus \bigoplus_{v \in V_{K,f}} \mathbb{Q}/\mathbb{Z}.$$

We have a commutative diagram with exact rows and injective vertical maps, and the left square is cartesian:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Br}(L/K) & \xrightarrow{\oplus_v \mathrm{inv}_v} & \bigoplus_v \frac{1}{[L_w:K_v]}\mathbb{Z}/\mathbb{Z} & \xrightarrow{\Sigma} & \frac{1}{N}\mathbb{Z}/\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Br}(K) & \xrightarrow{\oplus_v \mathrm{inv}_v} & R & \xrightarrow{\Sigma} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0
\end{array}$$

Proof. We already know we have such a commutative diagram with injective vertical maps. The fact that the left square is cartesian follows from the following observation: If $x \in \mathrm{Br}(K)$ is such that $\mathrm{inv}_v(x) \in \frac{1}{[L_w:K_v]}\mathbb{Z}/\mathbb{Z}$ for all v, then restriction to $\mathrm{Br}(L)$ kills all local invariants of x and hence kills x, and so $x \in \mathrm{Br}(L/K)$.

For the exactness of both rows, only the condition that $\ker(\Sigma) \subset \mathrm{im}(\bigoplus_v \mathrm{inv}_v)$ for each row is unknown. This condition for the first row follows from this condition for the second row plus the fact that the left square is cartesian. It remains to check that the second row is exact. Under the isomorphisms $\bigoplus_v \mathrm{inv}_v : \mathrm{Br}_A(K) \xrightarrow{\sim} R$ and $\mathrm{inv} : \mathrm{Br}_C(K)_{\mathrm{reg}} \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$, this row is isomorphic to the exact sequence $0 \to \mathrm{Br}(K) \to \mathrm{Br}_A(K) \to \mathrm{Br}_C(K)_{\mathrm{reg}} \to 0$. □

Theorem 2.9.3. *We have* $\mathrm{Br}_C(K)_{\mathrm{reg}} = \mathrm{Br}_C(K)$*. For every finite Galois L/K, the restriction of* $\mathrm{inv} : \mathrm{Br}_C(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ *to* $\mathrm{Br}(L/K)$ *induces an isomorphism* $\mathrm{Br}_C(L/K) \xrightarrow{\sim} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$*.*

Proof. By the compatibility of local invariants with restriction and by the fact that $\sum_{w|v}[L_w : K_v] = [L : K]$, we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Br}_A(K) & \xrightarrow{\mathrm{inv}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle [L:K]} \\ \mathrm{Br}_A(L) & \xrightarrow{\mathrm{inv}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

Thus we also have a similar commutative diagram with $\mathrm{Br}_A(\cdot)$ replaced by $\mathrm{Br}_C(\cdot)_{\mathrm{reg}}$. Let $\Phi = \ker(\mathrm{Res} : \mathrm{Br}_C(K)_{\mathrm{reg}} \to \mathrm{Br}_C(L)_{\mathrm{reg}})$. Then $\mathrm{inv} : \mathrm{Br}_C(K)_{\mathrm{reg}} \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ restricts to an isomorphism $\Phi \xrightarrow{\sim} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$. On the other hand we have $\Phi = \mathrm{Br}_C(K)_{\mathrm{reg}} \cap \mathrm{Br}_C(L/K)$ since we have the inflation-restriction exact sequence $0 \to \mathrm{Br}_C(L/K) \to \mathrm{Br}_C(K) \to \mathrm{Br}_C(L)$ (coming from the inflation-restriction exact sequences at finite stages, which are due to the vanishing of $\mathbf{H}^1$ of the idele class group). But by the Second Inequality we have $|\mathrm{Br}_C(L/K)| \leq [L : K]$, so we must have $\mathrm{Br}_C(L/K) = \Phi$, i.e., $\mathrm{Br}_C(L/K) \subset \mathrm{Br}_C(K)_{\mathrm{reg}}$. Since this holds for all L/K, we have $\mathrm{Br}_C(K)_{\mathrm{reg}} = \mathrm{Br}_C(K)$. □

We have finally verified the assumptions in Tate's theorem. Let L/K be a finite Galois extension, and let $u = u_{L/K}$ be the canonical generator of $\mathrm{Br}(L/K)$ such that $\mathrm{inv}(u) = 1$. Then Tate's theorem yields that cupping with u is an isomorphism

$$\widehat{\mathbf{H}}^q(\mathrm{Gal}(L/K), \mathbb{Z}) \xrightarrow{\sim} \widehat{\mathbf{H}}^{q+2}(\mathrm{Gal}(L/K), C_L).$$

In particular, for $q = 2$ we obtain an isomorphism

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} \xrightarrow{\sim} C_K/\mathrm{N}_{L/K}C_L.$$

For L/K finite abelian, the global Artin map $\psi_{L/K} : C_K \to \mathrm{Gal}(L/K)$ which we defined earlier using local-global compatibility satisfies the characterization $\chi(\psi_{L/K}(a)) = \sum_v \mathrm{inv}_v(\bar{a} \cup \delta\chi) = \mathrm{inv}(\bar{a} \cup \delta\chi)$, as shown in the proof of Lemma 2.8.2. The inverse of the isomorphism yielded by Tate's theorem satisfies the same characterization, by the same argument as the proof of Lemma 1.24.3. Hence the two ways of defining the global Artin map agree. Moreover, norm and transfer functoriality are proved in exactly the same way as in local class field theory, using the above characterization of the global Artin map in terms of inv and using the functoriality properties of inv. We leave the details to the reader.

At this point, all the desired statements in global class field theory are proved except the Existence Theorem (Theorem 2.1.3).

2.10. **Proof of the Existence Theorem.** Let K be a global field. Our goal is to prove Theorem 2.1.3. We follow [Mil20] to use the Norm Limitation Theorem to simplify the proof in [CF+67, §VII.12]. The characteristic p case of the proof (more specifically, this case of Lemma 2.10.8) is not found in either reference.

Definition 2.10.1. A subgroup of C_K is called *normic* if it is of the form $\mathrm{N}_{L/K}(C_L)$ for a finite abelian extension L/K.

By Remark 2.1.4, in order to prove Theorem 2.1.3 we only need to prove:

Theorem 2.10.2. *Every finite index open subgroup of C_K is normic.*

Before proving Theorem 2.10.2, we first discuss a separate result, called the Norm Limitation Theorem. This will simplify our proof and is itself an interesting result.

The basic observation is the following: As we have already verified all assumptions in Tate's theorem, we know that for every finite Galois extension L/K (not necessarily abelian) we have an isomorphism given by cupping with the fundamental class:

$$\widehat{\mathbf{H}}^{-2}(\mathrm{Gal}(L/K),\mathbb{Z}) \xrightarrow{\sim} C_K/\mathrm{N}_{L/K}(C_L).$$

But the left hand side is $\mathrm{Gal}(L/K)^{\mathrm{ab}}$, and it depends only on the maximal abelian subextension M/K inside L/K. In particular, if we replace L by M, then the left hand side does not change. It easily follows that we have

$$\mathrm{N}_{L/K}(C_L) = \mathrm{N}_{M/K}(C_M).$$

This phenomenon can be called "norm limitation"—it tells us that it is impossible to classify all finite Galois extensions L of K just by looking at $\mathrm{N}_{L/K}(C_L)$, as the latter cannot distinguish between an extension and its maximal abelian subextension. By pushing this idea slightly further, we get the following more general statement:

Theorem 2.10.3 (Norm Limitation Theorem)**.** *Let E/K be a finite separable extension. Let M/K be the maximal abelian (Galois) subextension of E/K. Then $\mathrm{N}_{E/K}(C_E) = \mathrm{N}_{M/K}(C_M)$.*

Proof. Let L/K be a finite Galois extension containing E. Let $G = \mathrm{Gal}(L/K), H = \mathrm{Gal}(L/E)$. Since M/K is the maximal subextension of L/K which is abelian and contained in E, $\mathrm{Gal}(L/M)$ is the smallest normal subgroup of G which contains $[G,G]$ and H. Note that $[G,G]H$ is a normal subgroup of G, as it is the preimage of the image of H in G^{ab}. Hence $\mathrm{Gal}(L/M) = [G,G]H$. It follows that we have a short exact sequence of abelian groups

$$H^{\mathrm{ab}} \xrightarrow{i} G^{\mathrm{ab}} \to \mathrm{Gal}(M/K) \to 0,$$

where i is induced by the inclusion $H \hookrightarrow G$ and the second map is induced by the projection $G \to \mathrm{Gal}(M/K)$. On the other hand, by norm functoriality of the isomorphism given by cupping with the fundamental class, we have a commutative diagram

$$\begin{array}{ccc} H^{\mathrm{ab}} & \xrightarrow{\cong} & C_E/\mathrm{N}_{L/E}(C_L) \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \mathrm{N}_{E/K}} \\ G^{\mathrm{ab}} & \xrightarrow{\cong} & C_K/\mathrm{N}_{L/K}(C_L) \end{array}$$

Thus $|C_K/\mathrm{N}_{E/K}(C_E)| = |\operatorname{Cok} i| = |\mathrm{Gal}(M/K)| = |C_K/\mathrm{N}_{M/K}(C_M)|$. Hence $\mathrm{N}_{E/K}(C_E) = \mathrm{N}_{M/K}(C_M)$ since we have $\mathrm{N}_{E/K}(C_E) \subset \mathrm{N}_{M/K}(C_M)$. □

Remark 2.10.4. The same proof also works for local fields. Thus for a finite separable extension of local fields E/K with maximal abelian subextension M/K, we have $\mathrm{N}_{E/K}(E^\times) = \mathrm{N}_{M/K}(M^\times)$.

Example 2.10.5. Let E/K be a prime degree separable extension which is not Galois. Then there is no non-trivial Galois extension of K inside E. Hence we have $\mathrm{N}_{E/K}C_E = C_K$ in the global case and $\mathrm{N}_{E/K}E^\times = K^\times$ in the local case.

We now prove three lemmas as preparation for proving Theorem 2.10.2.

Lemma 2.10.6. *Let H be a subgroup of C_K containing a normic subgroup. Then H is normic.*

Proof. Let L/K be a finite abelian extension such that $H \supset \mathrm{N}_{L/K}C_L$. Let H' be the image of $H/\mathrm{N}_{L/K}C_L$ under the Artin isomorphism $C_K/\mathrm{N}_{L/K}C_L \xrightarrow{\sim} \mathrm{Gal}(L/K)$. Let $E = L^{H'}$. Then H is the kernel of the composite map $C_K \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$. But this kernel is $\mathrm{N}_{E/K}C_E$, so H is normic. □

Lemma 2.10.7. *Let K'/K be a finite separable extension. Let H be a subgroup of C_K such that $\mathrm{N}^{-1}_{K'/K}(H)$ is a normic subgroup of $C_{K'}$. Then H is normic.*

Proof. Let L/K' be a finite abelian extension such that $\mathrm{N}^{-1}_{K'/K}(H) = \mathrm{N}_{L/K'}C_L$. Then $H \supset \mathrm{N}_{K'/K}(\mathrm{N}_{L/K'}C_L) = \mathrm{N}_{L/K}C_L$. Since L/K is a finite separable extension, $\mathrm{N}_{L/K}C_L$ is a normic subgroup of C_K by Theorem 2.10.3. It then follows from Lemma 2.10.6 that H is normic. □

Lemma 2.10.8. *Let H be an open subgroup of C_K of index a prime p. If $p \neq \mathrm{char}(K)$, we assume that $K \supset \mu_p$. Then H is normic.*

Proof. The proofs in the two cases $\mathrm{char}(K) \neq p$ and $\mathrm{char}(K) = p$ both refer back to some key results established during the proof of the Second Inequality in the respective case.

First consider the case $\mathrm{char}(K) \neq p$ and $K \supset \mu_p$. Let S be a finite subset of V_K containing $V_{K,\infty}$ and all places dividing p and such that $\mathbb{A}_K^\times = K^\times \mathbb{A}_{K,S}^\times$. (See the discussion below Fact 2.3.4.) Up to enlarging S, we may also assume that the inverse image of H in $\mathbb{A}_K^\times$ contains $\prod_{v\in S}\{1\} \times \prod_{v\notin S} \mathcal{O}_{K_v}^\times$. (Here we used the openness of H.) Let $M = K(\sqrt[p]{a}, a \in \mathcal{O}_{K,S}^\times)$, and let $E = \prod_{v\in S}(K_v^\times)^p \times \prod_{v\notin S} \mathcal{O}_{K_v}^\times \subset \mathbb{A}_K^\times$, with image $\bar{E}$ in C_K. Thus by our last assumption on S we have $H \supset \bar{E}$. Now by exactly the same arguments as in the proof of Theorem 2.4.2 in the $\mathrm{char}(K) \neq p$ case (see §2.4), we have $\bar{E} \subset \mathrm{N}_{M/K}C_M$ and $[C_K : \bar{E}] = p^{|S|}$. (Roughly speaking, one specializes that proof to the case $L = M$ and $T = \emptyset$.) But we also know that $[C_K : \mathrm{N}_{M/K}C_M] = [M : K]$ and this is $p^{|S|}$ by Kummer theory. Hence $\bar{E} = \mathrm{N}_{M/K}C_M$. Since $H \supset \bar{E}$, H is normic by Lemma 2.10.6.

Now consider the case $\mathrm{char}(K) = p$. Recall from §2.5 that we have a canonical isomorphism of topological groups $\Phi : C_K/C_K^p \xrightarrow{\sim} \mathrm{Gal}(M/K)$, where M/K is the maximal Artin–Schreier extension. In the proof of Theorem 2.4.2 in the $\mathrm{char}(K) = p$ case (see the end of §2.5), we showed that for any degree p extension L/K inside M/K, if R denotes the image of $(\mathrm{N}_{L/K}C_L)/C_K^p$ under Φ, then $M^R = L$ or K. Now we know that $\mathrm{N}_{L/K}C_L$ has index $p > 1$ in C_K, so $R \subsetneq \mathrm{Gal}(M/K)$ and $M^R = L$. Therefore $R = \mathrm{Gal}(M/L)$. Now $\Phi(H/C_K^p)$ is an open index p subgroup of $\mathrm{Gal}(M/K)$ by our assumption on H. Hence it is of the form $\mathrm{Gal}(M/L)$ for some degree p extension L/K inside M. By what we just recalled, $\Phi((\mathrm{N}_{L/K}C_L)/C_K^p) = \mathrm{Gal}(M/L) = \Phi(H/C_K^p)$. It follows that $H = \mathrm{N}_{L/K}C_L$. □

Proof of Theorem 2.10.2. We prove by induction on $n \geq 1$ that for every global field K and every open subgroup H of C_K of index $\leq n$, H is normic. If $[C_K : H] = 1$, there is nothing to prove. Suppose $[C_K : H] > 1$. Take a prime p dividing $[C_K : H]$. If $\mathrm{char}(K) \neq p$ and K does not contain the primitive p-th roots of unity, let $K' = K(\zeta_p)$. Since K'/K is finite separable, by Lemma 2.10.7 we can replace (K, H) by $(K', H' = \mathrm{N}^{-1}_{K'/K}(H))$. Note that $[C_{K'} : H'] \leq [C_K : H]$. If we have strict inequality, then the proof is finished by induction hypothesis. Thus we may assume that $[C_{K'} : H'] = [C_K : H]$.

In conclusion, we have reduced to the case where there is a prime p dividing $[C_K : H]$ and either $\mathrm{char}(K) = p$ or $\mathrm{char}(K) \neq p$ and $K \supset \mu_p$. Since C_K/H is a finite abelian group of order divisible by p, there is an index p subgroup H_1 of C_K containing H. Since H is open, so is H_1. By Lemma 2.10.8, there is a finite abelian extension L/K such that

$H_1 = \mathrm{N}_{L/K} C_L$. Let $H' = \mathrm{N}_{L/K}^{-1}(H)$. Then we have an injection $\mathrm{N}_{L/K} : C_L/H' \hookrightarrow C_K/H$, whose image is H_1/H. Thus $[C_L : H'] = [H_1 : H] = [C_K : H]/p$, so by induction hypothesis H' is normic in C_L. Then by Lemma 2.10.7 H is normic. □

3. Applications

3.1. **Hasse principle for quadratic forms.** We would like to study the problem of representing numbers by quadratic forms. Let K be a field of characteristic different from 2, which for us will be either a global or local field. Let $Q(X_1, \ldots, X_n)$ be a homogeneous quadratic polynomial $\sum_{i,j} a_{ij} X_i X_j$ over K, and let $c \in K$. The question is whether the equation

$$Q(X_1, \ldots, X_n) = c$$

has a solution $x_1, \ldots, x_n \in K$ such that x_i are not all zero. (The last requirement is to rule out the trivial solution in the case $c = 0$.) When there is such a solution we say that the quadratic form Q *represents* c.

We first recall the notion of a quadratic form.

Definition 3.1.1. Let K be a field. A quadratic form Q on a finite dimensional K-vector space V is a function $Q : V \to K$ satisfying:

(1) $Q(av) = a^2 Q(v)$ for all $a \in K, v \in V$.
(2) The map $B(v, w) = Q(v + w) - Q(v) - Q(w)$ is a bilinear form on V (i.e., a linear map $V \otimes_K V \to V$). We call it the bilinear form associated with Q.

If B is non-degenerate, then we call Q non-degenerate. Two quadratic forms Q, Q' on V are said to be *equivalent*, if there is a K-linear automorphism $\phi : V \to V$ such that $Q(v) = Q'(\phi(v))$ for all $v \in V$. We also call the pair (V, Q) a *quadratic space*.

Remark 3.1.2. We have $B(v, v) = Q(2v) - 2Q(v) = 2Q(v)$. Hence if $\mathrm{char} K \neq 2$ then Q is uniquely determined by B by $Q(v) = \frac{1}{2} B(v, v)$. We will only focus on this case, and hence the theory of quadratic forms is equivalent to the theory of bilinear forms.

We will often fix a basis $\{e_1, \ldots, e_n\}$ of V and then think of a quadratic form Q on V as a homogeneous quadratic polynomial $Q(X_1, \ldots, X_n)$, i.e.,

$$Q(X_1, \ldots, X_n) := Q(X_1 e_1 + \cdots + X_n e_n) \in K[X_1, \ldots, X_n].$$

This polynomial is well defined up to an invertible linear change of variables

$$X_i = \sum_j a_{ij} X'_j, \quad (a_{ij}) \in \mathrm{GL}_n(K).$$

We will call two homogeneous quadratic polynomials related by such a change of variables *equivalent*. Note that two quadratic forms Q and Q' on V are equivalent if and only if the equivalence class of quadratic polynomials associated with Q is the same as that associated with Q'. In the following, we will not distinguish between an equivalence class of quadratic forms with an equivalent class of homogeneous quadratic polynomials. Since for most of the time we will only consider quadratic forms up to equivalence, the vector space V is of minor importance and will often be omitted.

The following result is well known from linear algebra:

Lemma 3.1.3. *If* $\mathrm{char} K \neq 2$, *then up to equivalence every quadratic form can be written as* $Q(X_1, \ldots, X_n) = a_1 X_1^2 + \cdots + a_n X_n^2$ *for* $a_i \in K$.

Proof. We know every bilinear form can be diagonalized. □

From now on, we always assume that char$K \neq 2$.

Definition 3.1.4. We say a quadratic form Q on V represents $c \in K$ if there exists $v \in V - \{0\}$ such that $Q(v) = c$. Equivalently, there exist $x_1, \dots, x_n \in K$ not all zero such that $Q(x_1, \dots, x_n) = c$.

Clearly the set of $c \in K$ represented by Q depends only on the equivalence class of Q.

Remark 3.1.5. A quadratic form Q on an n-dimensional vector space is degenerate if and only if in the diagonal form $Q(X_1, \dots, X_n) = a_1X_1^2 + \cdots + a_nX_n^2$ at least one a_i is zero. Suppose this is the case. Up to reordering assume $a_1, \dots, a_k$ are non-zero and $a_{k+1} = \cdots = a_n = 0$. Then we can view Q as a non-degenerate quadratic form in k variables $Q'(X_1, \dots, X_k) = a_1X_1^2 + \cdots + a_kX_k^2$. Clearly, an element $c \in K^\times$ is represented by Q if and only if it is represented by Q'. However, whether 0 is represented is changed: The original degenerate Q always represents 0 since $Q(0, \dots, 0, 1, \dots, 1) = 0$ (with the first k variables being 0), but the new non-degenerate form $Q'(X_1, \dots, X_k)$ may or may not represent 0 (since by our definition representing 0 means $Q'(x_1, \dots, x_k) = 0$ for $x_1, \dots, x_k \in K$ *not all zero*). Thus in the study of whether a quadratic form represents 0 the degenerate case is uninteresting. Without any loss of generality, we shall exclusively consider non-degenerate quadratic forms in the study of the representation problem.

We have the following observation:

Lemma 3.1.6. *A non-degenerate quadratic form Q over K represents 0 if and only if it represents all $c \in K$.*

Proof. Let $B(v, w)$ be the associated bilinear form. Suppose $Q(v) = 0$ for $v \in V - \{0\}$. For $w \in V$ and $t \in K$, we have

$$Q(tv + w) = Q(tv) + Q(w) + B(tv, w) = t^2Q(v) + Q(w) + tB(v, w) = Q(w) + tB(v, w).$$

Since B is non-degenerate and $v \neq 0$, we can find $w \in V - \{0\}$ such that $B(v, w) \neq 0$. Then letting $t = B(v, w)^{-1}(c - Q(w))$, we obtain $Q(tv + w) = c$. □

Example 3.1.7. The quadratic form $X^2 - Y^2$ represents 0 since $1^2 - 1^2 = 0$. Hence it represents all $c \in K$. Indeed, $(\frac{c+1}{2})^2 - (\frac{c-1}{2})^2 = c$.

The following lemma reduces the question of whether a non-degenerate quadratic form represents a particular $c \in K$ to the question of whether a (possibly different) non-degenerate quadratic form represents 0.

Lemma 3.1.8. *A non-degenerate quadratic form $Q(X_1, \dots, X_n)$ represents $c \in K^\times$ if and only if the non-degenerate quadratic form in $n + 1$ variables $R(X_1, \dots, X_n, Y) = Q(X_1, \dots, X_n) - cY^2$ represents 0.*

Proof. If $Q(x_1, \dots, x_n) = c$, then $R(x_1, \dots, x_n, 1) = 0$. Conversely, assume $R(x_1, \dots, x_n, y) = 0$ with $\{x_1, \dots, x_n, y\}$ not all zero. If $y = 0$, then $Q(x_1, \dots, x_n) = R(x_1, \dots, x_n, y) = 0$, and x_i are not all zero. Thus Q represents 0, and so by Lemma 3.1.6 it represents c. If $y \neq 0$, then from $Q(x_1, \dots, x_n) = cy^2$ we obtain $Q(x_1/y, \dots, x_n/y) = c$, and x_i/y are not all zero since $c \neq 0$. □

Example 3.1.9. In the field K, -1 is a square if and only if the quadratic form X^2 represents -1, and by the above lemma this is equivalent to the condition that $X^2 + Y^2$ represents 0.

In order to study whether a non-degenerate quadratic form Q represents 0, we may write Q in diagonal form and also multiply it by an element of $K^\times$ to assume that one of the coefficients is 1. Thus without loss of generality we may assume $Q(X_1, \ldots, X_n) = X_1^2 + a_2X_2^2 + \ldots + a_nX_n^2$. (By non-degeneracy, every $a_i \in K^\times$.) For $n \leq 4$, whether such Q represents 0 is decided by whether a certain field element is a square or a norm from an extension, as follows:

Lemma 3.1.10. *Let $b, c, d \in K^\times$.*

(1) *($n = 1$.) The quadratic form X_1^2 does not represent 0.*
(2) *($n = 2$.) The quadratic form $X_1^2 - bX_2^2$ represents 0 if and only if $b \in (K^\times)^2$.*
(3) *($n = 3$.) The quadratic form $X_1^2 - bX_2^2 - cX_3^2$ represents 0 if and only if c is a norm from $K(\sqrt{b})$.*
(4) *($n = 4$.) The following statements are equivalent:*
   (a) *The quadratic form $X_1^2 - bX_2^2 - cX_3^2 + cdX_4^2$ represents 0.*
   (b) *c can be written as c_1c_2 where $c_1 \in K^\times$ is a norm from $K(\sqrt{d})$ and $c_2 \in K^\times$ is a norm from $K(\sqrt{b})$.*
   (c) *c lies in the image of the norm map $K(\sqrt{b}, \sqrt{d})^\times \to K(\sqrt{bd})^\times$.*
   (d) *The quadratic form $X_1^2 - bX_2^2 - cX_3^2$, viewed as a non-degenerate quadratic form in three variables over $K(\sqrt{bd})$, represents 0.*

Proof. Only (4) is non-obvious. The equivalence between (c) and (d) follows from (3). We prove (4) only under the assumption that b and d are non-squares in K. (The other cases are easier and left to the reader.)

Suppose $x_1, \ldots, x_4 \in K$ are not all zero and $x_1^2 - bx_2^2 - cx_3^2 + cdx_4^2 = 0$, i.e.,

$$x_1^2 - bx_2^2 = cx_3^2 - cdx_4^2.$$

If $x_1^2 - bx_2^2$ and $cx_3^2 - cdx_4^2$ are both 0, then by our assumption that b and d are non-squares we have $x_1 = x_2 = x_3 = x_4 = 0$, a contradiction. Hence $x_1^2 - bx_2^2$ and $cx_3^2 - cdx_4^2$ are both non-zero. Then

$$c = (x_1 - bx_2^2)(x_3^2 - dx_4^2)^{-1},$$

and these two factors are norms from $K(\sqrt{b})$ and $K(\sqrt{d})$ respectively. Hence (a) implies (b). The above arguments can be reversed, so (b) also implies (a).

It remains to prove that (b) is equivalent to (c). If bd is a square, then $K(\sqrt{b}, \sqrt{d}) = K(\sqrt{b}) = K(\sqrt{d})$ and $K(\sqrt{bd}) = K$, so (b) and (c) are trivially equivalent. Assume that bd is not a square. Then we have $\mathrm{Gal}(K(\sqrt{b}, \sqrt{d})/K) = \{1, \sigma, \tau, \sigma\tau\}$, where

$$\sigma(\sqrt{b}) = -\sqrt{b}, \quad \sigma(\sqrt{d}) = \sqrt{d},$$
$$\tau(\sqrt{b}) = \sqrt{b}, \quad \tau(\sqrt{d}) = -\sqrt{d}.$$

A general element of $K(\sqrt{b}, \sqrt{d})$ is of the form

$$r + s\sqrt{b} + t\sqrt{d} + u\sqrt{bd}$$

with $r, s, t, u \in K$ and its norm to $K(\sqrt{bd}) = K(\sqrt{b}, \sqrt{d})^{\{1,\sigma\tau\}}$ is

$$(r + s\sqrt{b} + t\sqrt{d} + u\sqrt{bd})(r - s\sqrt{b} - t\sqrt{d} + u\sqrt{bd}) = r^2 - s^2b - t^2d + u^2bd + (2ru - 2st)\sqrt{bd}$$

If we set $t = u = 0$, then we obtain $r^2 - s^2b$, which is a general element of $\mathrm{N}_{K(\sqrt{b})/K}(K(\sqrt{b}))$. Similarly, setting $s = u = 0$ we obtain a general element of $\mathrm{N}_{K(\sqrt{d})/K}(K(\sqrt{d}))$. Hence (b)

implies (c). Conversely, assume (c). Then since $c \in K$, by the above computation we know that c is of the form

$$c = r^2 - s^2 b - t^2 d + u^2 bd$$

with $r, s, t, u \in K$ and $ru = st$ (since the term $(2ru - 2st)\sqrt{bd}$ must be zero).

If $u = 0$, then one of s, t is 0, so c is either a norm from $K(\sqrt{d})$ or a norm from $K(\sqrt{b})$, and we have proved (b).

Assume $u \neq 0$. Then $r = u^{-1}st$, and we compute

$$(s^2 - u^2 d)(t^2 - u^2 b) = s^2 t^2 - s^2 u^2 b - t^2 u^2 d + u^4 bd = u^2 c.$$

Set $c_1 = (s/u)^2 - d \in \mathrm{N}_{K(\sqrt{d})/K}(K(\sqrt{d}))$ and $c_2 = (t/u)^2 - b \in \mathrm{N}_{K(\sqrt{b})/K}(K(\sqrt{b}))$. Then $c = c_1 c_2$, so (b) holds. □

Exercise 3.1.11. Prove Lemma 3.1.10 (4) when at least one of b and d is a square.

Lemma 3.1.12 (Weak approximation)**.** *Let K be a global field, and S a finite subset of V_K. Let U_v be a non-empty open subset of $K_v^\times$ for each $v \in S$. Then there exists $x \in K^\times$ such that $x \in U_v \subset K_v^\times$ for all $v \in S$.*

Proof. Without loss of generality we may assume that $S \supset V_{K,\infty}$. Recall that $\prod'_{v \in V_K - S} K_v^\times$ has dense image in C_K. Hence the open subset $\prod_{v \in S} U_v \times \prod_{v \notin S} \mathcal{O}_{K_v}^\times \subset \mathbb{A}_K^\times$ contains an element of the form xa, where $x \in K^\times$ and a is an idele whose coordinates at all $v \in S$ are 1. It follows that $x \in U_v$ for all $v \in S$. □

Theorem 3.1.13 (Hasse Principle)**.** *Let Q be a non-degenerate quadratic form in $n \geq 2$ variables over a global field K whose characteristic is not 2. Then Q represents 0 over K if and only if Q represents 0 over K_v (i.e., $Q(x_1, \ldots, x_n) = 0$ for some $x_i \in K_v$ not all zero) for all $v \in V_K$.*

Proof. The "only if" direction is trivial. For the "if" direction, when $n = 2, 3, 4$, by Lemma 3.1.10 we know that whether Q represents 0 depends on whether a certain element of K or $K(\sqrt{bd})$ is a square or a norm from a quadratic extension $K(\sqrt{b})/K$ or $K(\sqrt{b}, \sqrt{d})/K(\sqrt{bd})$. Such a problem satisfies local-global principle. Indeed, for being a square, suppose $b \in K^\times$ is not a square in K. Then $K(\sqrt{b})/K$ is a non-trivial quadratic extension and hence there are infinitely many places of K which are non-split in $K(\sqrt{b})$ by Corollary 2.3.6. For such a place v, b cannot be a square in K_v.[8] For being a norm from a cyclic extension, we have local-global principle by the Hasse Norm Theorem (Theorem 2.7.6). Therefore the "if" direction holds.

For $n \geq 5$, we prove the "if" direction by induction. We may assume that Q is in diagonal form, and write

$$Q(X_1, \ldots, X_n) = a_1 X_1^2 + a_2 X_2^2 - P(X_3, \ldots, X_n)$$

where P is a non-degenerate quadratic form in $n - 2$ variables. Write $P(X_3, \ldots, X_n) = \sum_{i=3}^n b_i X_i^2$, with all $b_i \in K^\times$. If $v \in V_K$ is such that P does not represent 0 over K_v, then the three-variable non-degenerate $b_3 X_3^2 + b_4 X_4^2 + b_5 X_5^2$ does not represent 0 over K_v, and by Lemma 3.1.10 v is a place where $-b_5/b_3 \in K^\times$ is not a local norm from $K(\sqrt{-b_4/b_3})$. We conclude that the set S of $v \in V_K$ such that P does not represent 0 over K_v is finite. Let $v \in S$. By assumption Q represents 0 over K_v, so there exist $x_1(v), x_2(v) \in K_v$ such that $z(v) := a_1 x_1(v)^2 + a_2 x_2(v)^2$ is non-zero and P represents $z(v)$ over K_v. Since $z(v)(K_v^\times)^2$ is an open neighborhood of $z(v)$ in $K_v^\times$ (since the characteristic is not 2), there exist an

[8] This is an "easy case" of the Grunwald–Wang theorem discussed last semester.

open neighborhood U_v of $x_1(v)$ and V_v of $x_2(v)$ such that for all $r \in U_v$ and $s \in V_v$ we have $a_1r^2 + a_2s^2 \in z(v)(K_v^\times)^2$. By Lemma 3.1.12, we find $x_1, x_2 \in K^\times$ such that $x_1 \in U_v$ and $x_2 \in V_v$ for all $v \in S$. Let $z = a_1x_1^2 + a_2x_2^2$. Then $z \in z(v)(K_v^\times)^2$ for all $v \in S$, and so P represents z over K_v for all $v \in S$, thanks to the fact that P represents $z(v)$. For $v \notin S$, P represents 0 over K_v by the definition of S, and so by Lemma 3.1.6 P represents all elements of K_v over K_v. Hence P represents z over all K_v. Equivalently, the $(n-1)$-variable $P(X_3, \dots, X_n) - zY^2$ represents 0 over all K_v (see Lemma 3.1.8). By induction hypothesis, $P(X_3, \dots, X_n) - zY^2$ represents 0 over K, or equivalently, P represents z over K. Thus $P(x_3, \dots, x_n) = z$ for some $x_3, \dots, x_n \in K$ not all zero. Then we have

$$Q(x_1, \dots, x_n) = z - z = 0.$$

□

Corollary 3.1.14. *Let Q be a non-degenerate quadratic form over a global field K whose characteristic is not 2, and let $c \in K$. Then Q represents c over K if and only if it represents c over K_v for all $v \in V_K$.*

Proof. This follows from Theorem 3.1.13 and Lemma 3.1.8. □

The Hasse Principle reduces the problem of representing 0 over a global field to representing 0 over a local field. For the latter problem we have the following result.

Proposition 3.1.15. *Let Q be a non-degenerate quadratic form in n variables over a local field K of whose characteristic is not 2.*

(1) *If $K = \mathbb{C}$, then Q represents 0.*
(2) *If $K = \mathbb{R}$, then Q represents 0 if and only if it is* indefinite, *i.e., if $Q = a_1X_1^2 + \cdots + a_nX_n^2$ then there is at least one positive a_i and one negative a_i.*
(3) *("Local Four Square Theorem") Let K be non-archimedean. If $n = 4$, then Q represents all elements of $K^\times$. If $n \geq 5$, then Q represents 0 and hence all elements of K.*

Proof. Only (3) is non-trivial. The first statement easily implies the second. We prove the first statement. Without loss of generality, we may assume that Q is of the form

$$Q(X_1, X_2, X_3, X_4) = X_1^2 - bX_2^2 - cX_3^2 + cdX_4^2.$$

Denote

$$N_b := \mathrm{N}_{K(\sqrt{b})/K}(K(\sqrt{b})^\times), \quad N_d := \mathrm{N}_{K(\sqrt{d})/K}(K(\sqrt{d})^\times)$$

Assume that Q does not represent every element of $K^\times$. Then by Lemma 3.1.8, Q does not represent 0. By Lemma 3.1.10, $c \notin N_b \cdot N_d$. It immediately follows that b and d are not squares in K.

If $K(\sqrt{b}) \neq K(\sqrt{d})$, then by local class field theory N_b and N_d are two distinct index 2 subgroups of $K^\times$, and it follows that $N_b \cdot N_d = K^\times$, contradicting with $c \notin N_b \cdot N_d$. Hence $K(\sqrt{b}) = K(\sqrt{d})$, or equivalently, $b \equiv d \mod (K^\times)^2$. Hence we may assume that $b = d$ (by rescaling X_4). Write N for $N_b = N_d$. Then

$$Q(x_1, x_2, x_3, x_4) = (x_1^2 - bx_2^2) - c(x_3^2 - bx_4^2), \quad x_1^2 - bx_2, x_3^2 - bx_4^2 \in N.$$

Thus it is clear that the set E of all elements of K represented by Q is

$$E = \{\alpha - c\beta \mid \alpha, \beta \in N \cup \{0\}, \text{ not both zero}\}.$$

By our assumption, E does not contain $K^\times$.

We have already seen that $c \notin N_b \cdot N_d$, i.e., $c \notin N$. Since $[K^\times : N] = 2$, we have $K^\times = N \sqcup cN$. If $-1 \in N$, then $E \supset N \cup cN = K^\times$, a contradiction. Hence $-1 \notin N$.

We claim that $N + 1 \subset N$. Suppose not. Let $\alpha \in N$ be such that $\alpha + 1 \notin N$. Since $-1 \notin N$, we have $\alpha \neq -1$, i.e., $\alpha + 1 \neq 0$. It follows that $\alpha + 1 \in cN$ since $K^\times = N \sqcup cN$. Write $\alpha + 1 = c\gamma$ with $\gamma \in N$. Then for any $u \in N$ we have

$$-u = \alpha u - c\gamma u \in E.$$

Hence E contains $N \cup (-N)$, which is $K^\times$ since $-1 \notin N$. A contradiction. The claim is proved.

Since N is an open subgroup of $K^\times$ (by the local reciprocity law), it contains $1 + \mathfrak{m}_K^r$ for sufficiently large r. Assume K is over $\mathbb{Q}_p$. Then N contains $1 - p^r \in \mathbb{Z}_{<0}$. By adding 1's to it and for $p^r - 2$ times and using the claim, we have $-1 \in N$, a contradiction. Assume that $\mathrm{char} K = p > 0$. Then $-1 = p - 1 = 1 + 1 + \cdots + 1 \in N$ by the claim, a contradiction. □

Corollary 3.1.16. *Let Q be a non-degenerate quadratic form in $n \geq 5$ variables over a global field K whose characteristic is not 2. Then Q represents 0 if and only if for every real place v of K, Q is indefinite over K_v.* □

Example 3.1.17. For any $c \in \mathbb{Q}_{>0}$, the non-degenerate quadratic form $X_1^2 + X_2^2 + X_3^2 + X_4^2 - cX_5^2$ over $\mathbb{Q}$ is indefinite over $\mathbb{R}$, and hence it represents 0. Thus c can be written as the sum of four squares in $\mathbb{Q}$. Similarly, for any quadratic form $P(X_1, \cdots, X_4)$ over $\mathbb{Q}$ which is not negative definite over $\mathbb{R}$, every $c \in \mathbb{Q}_{>0}$ can be represented by P over $\mathbb{Q}$.

3.2. **Hilbert symbol.** Fix an integer $m \geq 2$. Let K be a local field whose characteristic is coprime to m, and assume that $K \supset \mu_m$. Let M be the maximal Kummer extension of K in K^s with respect to m, i.e., $M = K(\sqrt[m]{a}, a \in K)$. Then by Kummer theory we have the pairing

$$K^\times/(K^\times)^m \times \mathrm{Gal}(M/K) \longrightarrow \mu_m, \quad (a, \sigma) \longmapsto \frac{\sigma \sqrt[m]{a}}{\sqrt[m]{a}}$$

(which is perfect in the sense of Pontryagin duality). We pre-compose this pairing with the local Artin map $\psi_K : K^\times/(K^\times)^m \to \mathrm{Gal}(M/K)$ (this factors through $K^\times/(K^\times)^m$ since the target is killed by m), and obtain the bi-multiplicative pairing

$$(\cdot, \cdot)_{K,m} : K^\times/(K^\times)^m \times K^\times/(K^\times)^m \longrightarrow \mu_m, \quad (a, b) \longmapsto \frac{\psi_K(b)\sqrt[m]{a}}{\sqrt[m]{a}}.$$

This is called the *Hilbert symbol* with respect to m. For simplicity we just write $(\cdot, \cdot)_K$.

Lemma 3.2.1. *For $a, b \in K^\times$, we have $(a, b)_K = 1$ if and only if b lies in $\mathrm{N}_{L/K}(L^\times)$ with $L = K(\sqrt[m]{a})$.*

Proof. Since L is generated by $\sqrt[m]{a}$, we have $(a, b)_K = 1$ if and only if $\psi_{L/K}(b) = 1 \in \mathrm{Gal}(L/K)$. But the kernel of $\psi_{L/K} : K^\times \to \mathrm{Gal}(L/K)$ is $\mathrm{N}_{L/K}(L^\times)$. □

Example 3.2.2. For $m = 2$, we have $(a, b)_K = 1$ if and only if the quadratic form $aX^2 + bY^2 - Z^2$ represents 0, by Lemmas 3.2.1 and 3.1.10. Note that this condition is symmetric in a and b. Since $(a, b)_K$ takes values only ± 1, we conclude that $(a, b)_K = (b, a)_K$ for all $a, b \in K^\times$. We will soon generalize this for general m. If $m = 2$ and $K = \mathbb{R}$, by the above condition in terms of quadratic form, we see that $(a, b)_K = -1$ if and only if $a < 0$ and $b < 0$.

Lemma 3.2.3. *For $a, b \in K^\times$, we have $(a, b)_K = 1$ if $a + b \in (K^\times)^m \cup \{0\}$.*

Proof. Write $a+b=c^m$ with $c\in K$. Let $L=K(\sqrt[m]{a})$. We need to show that $b\in \mathrm{N}_{L/K}(L^\times)$. Let H be the subgroup of $K^\times/(K^\times)^m$ generated by a. Fix a primitive m-th root of unity ζ. The pairing $H\times \mathrm{Gal}(L/K)\to \mu_m$ from Kummer theory is perfect. It follows that $\mathrm{Gal}(L/K)$ is cyclic, and there exists a generator σ of $\mathrm{Gal}(L/K)$ such that $\sigma\sqrt[m]{a}/\sqrt[m]{a}=\zeta^d$, where $d=m/|H|$. Then

$$b=c^m-a=\prod_{i=0}^{m-1}(c-\zeta^i\sqrt[m]{a})=\prod_{i=0}^{d-1}\prod_{j=0}^{\frac{m}{d}-1}(c-\zeta^{i+dj}\sqrt[m]{a})$$
$$=\prod_{i=0}^{d-1}\prod_{j=0}^{|H|}(c-\zeta^i\sigma^j\sqrt[m]{a})=\prod_{i=0}^{d-1}\mathrm{N}_{L/K}(c-\zeta^i\sqrt[m]{a})\in \mathrm{N}_{L/K}(L^\times).$$

□

Proposition 3.2.4 (Anti-symmetry of Hilbert symbol)**.** *We have* $(a,b)_K(b,a)_K=1$.

Proof. By Lemma 3.2.3, we have $(x,-x)_K=1$ for all $x\in K^\times$, and therefore by bi-multiplicativity we have

$$1=(ab,-ab)=(a,(-a)b)(b,a(-b))=(a,-a)(a,b)(b,a)(b,-b)=(a,b)(b,a).$$

□

Example 3.2.5. For $m=2$, we have $(a,b)_K=(b,a)_K$.

Proposition 3.2.6 (Product formula)**.** *Let K be a global field of characteristic coprime to m and containing μ_m. For all $a,b\in K^\times$, we have $(a,b)_{K_v,m}$ for almost all v, and*

$$\prod_{v\in V_K}(a,b)_{K_v,m}=1.$$

Proof. Let $L=K(\sqrt[m]{a})$. By the Local Reciprocity Law, the image of $b\in K^\times$ under the local Artin map $\psi_v:K_v^\times\to \mathrm{Gal}(L_w/K_v)\subset \mathrm{Gal}(L/K)$ is trivial if and only if $b\in \mathrm{N}_{L_w/K_v}(L_w^\times)$, and by Lemma 3.2.1 this is equivalent to $(a,b)_{K_v}=1$. Let S be the set of places of K satisfying these conditions. Then V_K-S is finite. By the Artin reciprocity law, i.e. statement (A) in Theorem 2.8.5, we have $\prod_{v\in V_K-S}\psi_v(b)=1$. On the other hand this Galois element sends $\sqrt[m]{a}$ to

$$\left(\prod_{v\in V_K-S}(a,b)_K\right)\sqrt[m]{a}=\left(\prod_{v\in V_K}(a,b)_K\right)\sqrt[m]{a}.$$

□

3.3. **Classification of quadratic forms over local and global fields.** We are interested in classifying all non-degenerate quadratic forms over a local or global field (of characteristic not 2) up to equivalence. Equivalently, we would like to classify non-degenerate quadratic spaces (V,Q) up to *isometry* (i.e. vector space isomorphisms preserving the quadratic forms). In the following, we will call the dimension of V the *rank* of Q, and we assume that all fields have characteristic not 2.

The first result is that the classification satisfies local-global principle.

Theorem 3.3.1 (Hasse–Minkowski)**.** *Let Q,Q' be non-degenerate quadratic forms over a global field K. Then Q and Q' are equivalent over K if and only if they are equivalent over K_v for all $v\in V_K$.*

For the proof, we need a special case of Witt's theorem. First we discuss orthogonal decomposition. In an Euclidean space V (i.e., positive definite quadratic space over $\mathbb{R}$), for any subspace U we have an orthogonal decomposition $V = U \oplus U^\perp$. However this may not hold in a general non-degenerate quadratic space. Let (V, Q) be a non-degenerate quadratic space over a field K whose characteristic is not 2. Let B be the associated bilinear form. For any subspace $U \subset V$, define the *orthogonal complement*

$$U^\perp := \{v \in V \mid B(u, v) = 0, \forall u \in U\}.$$

Then $Q|_U$ is a non-degenerate quadratic form on U if and only if $U \cap U^\perp = 0$, if and only if $V = U \oplus U^\perp$. When this is the case, we call U a *non-degenerate subspace*. In this case, $U^\perp$ is also non-degenerate, so we have decomposed V into the orthogonal direct sum of two smaller non-degenerate quadratic spaces. For instance, if $\{e_1, \dots, e_n\}$ is an orthogonal basis and $1 \le i \le n$, then $U = \operatorname{span}\{e_1, \dots, e_i\}$ is a non-degenerate subspace with $U^\perp = \operatorname{span}\{e_{i+1}, \dots, e_n\}$.

Note that V contains a degenerate subspace if and only if Q represents 0. Indeed, if $U \subset V$ is a degenerate subspace, then any $v \in U \cap U^\perp$ satisfies $Q(v) = 0$. Conversely, if $v \in V - \{0\}$ is such that $Q(v) = 0$, then $\operatorname{span}\{v\}$ is a degenerate subspace.

If we have two non-degenrate quadratic spaces $(V, Q), (V', Q')$ and orthogonal decompositions $V = U \oplus U^\perp, V' = U' \oplus (U')^\perp$, then for V to be isometric to V' it suffices that U is isometric to U' and $U^\perp$ is isometric to $(U')^\perp$.

Lemma 3.3.2 (Special case of Witt's theorem)**.** *Let $v, w \in V$ be such that $Q(v) = Q(w) \neq 0$. Then there exists an isometry between the non-degenerate quadratic spaces $v^\perp$ and $w^\perp$.*

Proof. We have $Q(v+w)+Q(v-w) = 4Q(v) \neq 0$, so at least one of $Q(v+w)$ and $Q(v-w)$ is non-zero. Up to replacing w by $-w$, we may assume that $Q(v - w) \neq 0$. Consider the reflection along $v - w$:

$$s : V \longrightarrow V, \quad u \mapsto u - \frac{B(u, v - w)}{Q(v - w)}(v - w).$$

In terms of the orthogonal decomposition $V = \langle v - w\rangle \oplus (v - w)^\perp$, the operator s is -1 on $\langle v - w\rangle$ and the identity on $(v - w)^\perp$. Clearly s is an isometry. We check that it sends v to w.[9] We compute

$$Q(v - w) = Q(v) + Q(w) - B(v, w) = 2Q(v) - B(v, w) = B(v, v) - B(v, w) = B(v, v - w).$$

Hence

$$s(v) = v - \frac{B(v, v - w)}{B(v, v - w)}(v - w) = v - (v - w) = w$$

as desired. Since $s : V \to V$ is an isometry sending v to w, it restricts to an isometry $v^\perp \xrightarrow{\sim} w^\perp$. □

Exercise 3.3.3. Prove the general form of Witt's theorem: Let $(V, Q), (V', Q')$ be two isometric non-degenerate quadratic spaces over a field of characteristic not 2. Let $U \subset V$ and $U' \subset V'$ be non-degenerate subspaces, and assume that there is an isometry $(U, Q|_U) \xrightarrow{\sim} (U', Q'|_{U'})$. Then there is an isometry $(U^\perp, Q|_{U^\perp}) \xrightarrow{\sim} ((U')^\perp, Q'|_{(U')^\perp})$.

[9] The geometric intuition is that $v, w, v - w$ are the three sides of an equilateral triangle with v and w the equal sides. Hence reflection along the direction $v - w$ must send v to w.

Proof of Theorem 3.3.1. The "only if" direction is obvious. We prove the "if" direction. If Q and Q' have rank 0, then there is nothing to prove. Assume that they have rank $n \geq 1$. Since Q is non-degenerate, it represents some $a \in K^\times$ over K. Then Q' represents a over K_v for all v, and so by Corollary 3.1.14 Q' represents a over K. Let V, V' be the K-vector spaces of Q, Q'. Thus there exist $v \in V$ and $v' \in V'$ such that $Q(v) = Q'(v') = a$. The quadratic spaces $v^\perp$ and $(v')^\perp$ over K are isometric over K_v for all v by Lemma 3.3.2. Then by induction on the rank, $v^\perp$ and $(v')^\perp$ are isometric over K. It follows that V and V' are isometric over K using the orthogonal decompositions $V = \langle v \rangle \oplus v^\perp$ and $V' = \langle v' \rangle \oplus (v')^\perp$. □

We now classify quadratic forms over a local field. Over $\mathbb{C}$, all non-degenerate quadratic forms of the same rank are equivalent. Over $\mathbb{R}$, we have Sylvester's theorem stating that every non-degenerate quadratic form is equivalent to $X_1^2 + \cdots + X_p^2 - Y_1^2 - \cdots - Y_q^2$ for a unique pair $(p, q) \in \mathbb{Z}^2_{\geq 0}$, called the *signature*. In the following consider a non-archimedean local field K (whose characteristic is not 2).

For a non-degenerate quadratic form $Q = \sum_{i=1}^n a_i X_i^2$ over K, we define two invariants:

- *Discriminant*: $d(Q) = \prod_i a_i \in K^\times/(K^\times)^2$.
- *Hasse invariant*: $\epsilon(Q) = \prod_{1 \leq i < j \leq n} (a_i, b_i)_K \in \{\pm 1\}$. Here $(\cdot,\cdot)_K = (\cdot,\cdot)_{K,2} : K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \to \{\pm 1\}$ is the Hilbert symbol with respect to 2.

To see that the discriminant is well defined (i.e., independent of the choice of an orthogonal basis), note that it is nothing but $2^{-n} \det A$, where A is the matrix of the bilinear form B associated to Q under the chosen orthogonal basis of V. If we change basis, then A is replaced by $P^t A P$ for some $P \in \mathrm{GL}_n(K)$, and we have $\det(P^t A P) = \det(P)^2 \det A = \det A \in K^\times/(K^\times)^2$. Clearly this works for any field K whose characteristic is not 2.

To see that the Hasse invariant is well defined, we need the following lemma:

Lemma 3.3.4. *Let (V, Q) be a non-degenerate quadratic space over a field K whose characteristic is not 2. Assume that $\dim V \geq 3$. Let $\mathcal{B}$ and $\mathcal{B}'$ be two orthogonal bases of V. Then there exists a chain $\mathcal{B}_0 = \mathcal{B}, \mathcal{B}_1, \ldots, \mathcal{B}_t = \mathcal{B}'$, where each $\mathcal{B}_i$ is an orthogonal basis of V, and for every i the two bases $\mathcal{B}_i$ and $\mathcal{B}_{i+1}$ share at least one common element.*

Proof. We write $\mathcal{B} \sim \mathcal{B}'$ if the conclusion of the lemma holds. Write $\mathcal{B} = \{e_1, \ldots, e_n\}, \mathcal{B}' = \{e_1', \ldots, e_n'\}$.

Case 1: There exists $1 \leq i \leq n$ such that $P = \mathrm{span}\{e_1, e_i'\}$ is a two-dimensional non-degenerate subspace. Without loss of generality, assume $i = 1$. We have $V = P \oplus P^\perp$, and $P^\perp$ is also non-degenerate. Let $\mathcal{C}$ be an orthogonal basis of $P^\perp$. Since $Q(e_1)$ and $Q(e_1')$ are non-zero, we can extend e_1 to an orthogonal basis $\{e_1, u\}$ of P, and extend e_1' to an orthogonal basis $\{e_1', v\}$ of P. Then we have (noting that $\mathcal{C} \neq \emptyset$)

$$\mathcal{B} \sim \{e_1, u\} \cup \mathcal{C} \sim \{e_1', v\} \cup \mathcal{C} \sim \mathcal{B}'.$$

Case 2: For all $1 \leq i \leq n$, $\mathrm{span}(e_1, e_i')$ is either one-dimensional or degenerate. Let B be the bilinear form associated with Q. Then our assumption concretely means that

$$B(e_1, e_1) B(e_i', e_i') = B(e_1, e_i')^2.$$

Note that the left hand is non-zero, so $B(e_1, e_i') \neq 0$.

We claim that there exists $x \in K$ such that $e_x := e_1' + x e_2'$ satisfies $Q(e_x) \neq 0$ and $\mathrm{span}\{e_1, e_x\}$ is two-dimensional and non-degenerate. We have

$$2Q(e_x) = B(e_x, e_x) = B(e_1', e_1') + x^2 B(e_2', e_2'),$$

so the condition $Q(e_x) \neq 0$ rules out at most two values of x. For $\mathrm{span}\{e_1, e_x\}$ to be two-dimensional and non-degenerate, we need

$$B(e_1, e_1)B(e_x, e_x) - B(e_1, e_x)^2 \neq 0.$$

We compute that the left hand side is equal to

$$\begin{aligned} &B(e_1, e_1)[B(e_1', e_1') + x^2 B(e_2', e_2')] - [B(e_1, e_1') + xB(e_1, e_2')]^2 \\ &\quad = B(e_1, e_1')^2 + x^2 B(e_1, e_2')^2 - [B(e_1, e_1') + xB(e_1, e_2')]^2 = -2xB(e_1, e_1')B(e_1, e_2'). \end{aligned}$$

Since $B(e_1, e_i') \neq 0$, for the above to be non-zero we only rule out $x = 0$. In conclusion, the conditions in the claim only rule out at most three values of x. If K is a field having at least four elements, then we are done. The only remaining case is when $K = \mathbb{F}_3$ (since its characteristic is not 2), which we leave as an exercise.

Now let x be as in the claim. Since $e_x \in \mathrm{span}\{e_1', e_2'\}$ and $Q(e_x) \neq 0$, we can extend e_x to an orthogonal basis $\{e_x, u\}$ of $\mathrm{span}\{e_1', e_2'\}$. Since $\mathrm{span}\{e_1, e_x\}$ is two-dimensional non-degenerate, by Case 1 already proved above, we have

$$\mathcal{B} \sim \{e_x, u, e_3', \dots, e_n'\}.$$

Since $n \geq 3$ we have $\{e_x, u, e_3', \dots, e_n'\} \sim \mathcal{B}'$. Hence $\mathcal{B} \sim \mathcal{B}'$. □

Exercise 3.3.5. Prove the claim in the above proof for $K = \mathbb{F}_3$.

Proposition 3.3.6. *The Hasse invariant is well defined.*

Proof. If the rank of Q is 2, then $\epsilon(Q) = 1$ if and only if Q represents 1 (see Example 3.2.2). This property is intrinsic to Q, independent of the choice of a basis. Assume the rank is at least 3. By Lemma 3.3.4, we only need to compare the definitions under two orthogonal bases of (V, Q) of the form $\{e_1, e_2, \dots, e_n\}$ and $\{e_1' = e_1, e_2', \dots, e_n'\}$. Let $a_i = Q(e_i)$ and $a_i' = Q(e_i')$. Thus we need to check that

$$A := \prod_{i<j} (a_i, a_j)_K$$

is equal to

$$A' := \prod_{i<j} (a_i', a_j')_K.$$

We have

$$A = \prod_{j \geq 2} (a_1, a_j)_K \cdot \prod_{2 \leq i < j} (a_i, a_j)_K = (a_1, d(Q)/a_1)_K \prod_{2 \leq i < j} (a_i, a_j)_K.$$

Similarly,

$$A' = (a_1, d(Q)/a_1)_K \prod_{2 \leq i < j} (a_i', a_j')_K$$

(since $a_1 = a_1'$). Thus it suffices to prove that

$$\prod_{2 \leq i < j} (a_i, a_j)_K = \prod_{2 \leq i < j} (a_i', a_j')_K.$$

But the two sides are the definitions of the Hasse invariant of the non-degenerate quadratic space $e_1^\perp$ under the two bases $\{e_2, \dots, e_n\}$ and $\{e_2', \dots, e_n'\}$. By induction on the rank, the Hasse invariant is well defined for $e_1^\perp$, so the two sides agree. □

Lemma 3.3.7. *Let Q be a non-degenerate quadratic form over a non-archimedean local field K of rank n. Let $b \in K^\times$. Then whether Q represents b depends only on the quadruple $(b, n, d(Q), \epsilon(Q))$. More precisely, we have:*

(1) *For $n = 1$, Q represents b if and only if $b = d(Q) \in K^\times/(K^\times)^2$.*
(2) *For $n = 2$, Q represents b if and only if $(b, -d(Q))_K = \epsilon(Q)$.*
(3) *For $n = 3$, Q represents b if and only if either $b \neq -d(Q)$, or $b = -d(Q)$ and $(-1, -d(Q))_K = \epsilon(Q)$. (Here the equality $b = -d(Q)$ is understood inside $K^\times/(K^\times)^2$.)*
(4) *For $n \geq 4$, Q always represents b.*

Proof. In the proof we write $(\cdot,\cdot)$ for the Hilbert symbol $(\cdot,\cdot)_K$. The case $n = 1$ is obvious. Let $n = 2$. Write $Q = a_1X_1^2 + a_2X_2^2$. Then Q represents b if and only if $b/a_1 = x_1^2 + (a_2/a_1)x_2^2$ for some $x_1, x_2 \in K$, if and only if b/a_1 is a norm from $K(\sqrt{-a_2/a_1})$, if and only if

$$(b/a_1, -a_2/a_1) = 1.$$

We have

$$(b/a_1, -a_2/a_1) = (b, -a_1a_2)(a_1, -a_1)(a_1, a_2) = (b, -d(Q))\epsilon(Q).$$

Hence Q represents b if and only if $(b, -d(Q)) = \epsilon(Q)$.

Let $n = 3$. Let $c \in K^\times$. Clearly Q represents b if and only if cQ represents cb. We check that the condition

$$b = -d(Q) \Rightarrow (-1, -d(Q)) = \epsilon(Q)$$

is also invariant under simultaneously scaling Q and b. Write $Q = a_1X_1^2 + a_2X_2^2 + a_3X_3^2$. Then

$$\begin{aligned}\epsilon(cQ) &= (ca_1, ca_2)(ca_1, ca_3)(ca_2, ca_3) = (ca_1, c^2a_2a_3)(ca_2, ca_3)\\ &= (ca_1, a_2a_3)(ca_2, ca_3) = (c, a_2a_3)(a_1, a_2a_3)(c, c)(c, a_3)(a_2, c)(a_2, a_3)\\ &= (c, a_2a_3)^2(c, c)\epsilon(Q) = (c, c)\epsilon(Q).\end{aligned}$$

We have

$$d(cQ) = c^3d(Q) = cd(Q).$$

Hence $b = -d(Q)$ if and only if $cb = -d(cQ)$. Also $(-1, -d(cQ)) = (-1, -cd(Q)) = (-1, c)(-1, -d(Q))$. This is equal to $\epsilon(cQ)$ if and only if $(-1, -d(Q)) = \epsilon(Q)$, because $(c, c) = (-c, c)(-1, c) = (-1, c)$.

Hence to prove the lemma for $n = 3$ we may simultaneously scale Q and b. Thus we may assume that Q is of the form $X_1^2 - cX_2^2 + cdX_3^2$ for some $c, d \in K^\times$. Then Q represents b if and only if the non-degenerate rank 4 quadratic form $X_1^2 - cX_2^2 + cdX_3^2 - bX_4^2$ represents 0. By Lemma 3.1.10, this holds if and only if $c = c_1c_2$ for $c_1 \in N_d := \mathrm{N}_{K(\sqrt{d})/K}(K(\sqrt{d})^\times)$ and $c_2 \in N_b := \mathrm{N}_{K(\sqrt{b})/K}(K(\sqrt{b})^\times)$. We have $d(Q) = -d$. If $b \neq -d(Q)$, then either N_b and N_d are two distinct index 2 subgroups of $K^\times$, or at least one of them is equal to $K^\times$, so in any case we have $c \in N_dN_b = K^\times$. Suppose $b = -d(Q)$. Then $N_b = N_d$, so Q represents b if and only if $c \in N_d$, if and only if $(c, d) = 1$. But $\epsilon(Q) = (-c, cd) = (-c, c)(-c, d) = (-c, d) = (-1, d)(c, d)$. So $\epsilon(Q) = (-1, -d(Q))$ if and only if $(c, d) = 1$, if and only if Q represents b.

The case $n \geq 4$ is already proved in Proposition 3.1.15. □

Exercise 3.3.8 (Theorem of three squares for rationals)**.** Let $b \in \mathbb{Q}_{>0}$. Using Corollary 3.1.14 and Lemma 3.3.7, prove that the following are equivalent:

(1) b cannot be written as $x^2 + y^2 + z^2$ for $x, y, z \in \mathbb{Q}$.
(2) $b \in -1 \cdot (\mathbb{Q}_2^\times)^2 \subset \mathbb{Q}_2^\times$.
(3) b is of the form $4^k\frac{u}{v}$ with $k \in \mathbb{Z}$, and u, v odd integers such that $uv^{-1} \equiv 7 \pmod 8$.

Hint: One can use the product formula to compute $(-1,-1)_{\mathbb{Q}_2}$.

Exercise 3.3.9 (Theorem of three squares for integers)**.** Suppose $b \in \mathbb{Z}_{\geq 1}$ can be written as the sum of three squares in $\mathbb{Q}$. Show that it can be written as the sum of three squares in $\mathbb{Z}$ in the following steps:

(1) Consider $S = \{x \in \mathbb{R}^3 \mid x \cdot x = b\}$. Suppose there is a point $x \in S \cap \mathbb{Q}^3$ and $x \notin \mathbb{Z}^3$. Then there exists $z \in \mathbb{Z}^3$ such that $(x-z)\cdot(x-z) < 1$. For such z, we have $(x-z)\cdot x \neq 0$, and so the line through x and z meets S in another point x'. We must have $x' \in \mathbb{Q}^3$.
(2) If $d \in \mathbb{Z}_{\geq 1}$ is such that $dx \in \mathbb{Z}^3$, then $d' := d(x-z)\cdot(x-z)$ satisfies: $d' \in \mathbb{Z}$, $1 \leq d' < d$, and $d'x' \in \mathbb{Z}^3$. (Hint: find a formula for x' in terms of x and z.)
(3) Conclude that if $S \cap \mathbb{Q}^3 \neq \emptyset$ then $S \cap \mathbb{Z}^3 \neq \emptyset$.

As an application, prove Gauss' theorem that every positive integer n can be written as

$$\sum_{i=1}^{3} \frac{n_i(n_i+1)}{2}, \quad n_i \in \mathbb{Z}_{\geq 0}$$

by applying the theorem of three squares to $8n+3$. Also show that every positive integer is either a sum of three squares in $\mathbb{Z}$, or the sum of three squares in $\mathbb{Z}$ plus a power of 4. (This is a more refined version of the usual theorem of four squares for integers.)

Theorem 3.3.10. *Let Q, Q' be two non-degenerate quadratic forms over a non-archimedean local field K of rank n. Then Q and Q' are equivalent if and only if $d(Q) = d(Q')$ and $\epsilon(Q) = \epsilon(Q')$.*

Proof. We have already seen the "only if" direction. We prove the "if" direction. If $n = 0$ then there is nothing to prove. Suppose $n \geq 1$. By Lemma 3.3.7, Q and Q' represent some common $b \in K^\times$, i.e., there exist $v \in (V, Q)$ and $v' \in (V', Q')$ such that $Q(v) = Q'(v') = b$. Let $\hat{Q} = Q|_{v^\perp}$. Extend v to an orthogonal basis $\{v, e_2, \dots, e_n\}$ of V, and let $a_i = Q(e_i)$. Then $d(Q) = b\prod_{i\geq 2} a_i = bd(\hat{Q})$, and

$$\epsilon(Q) = \prod_{i\geq 2}(b, a_i)_K \cdot \prod_{2\leq i<j}(a_i, a_j)_K = (b, d(Q)/b)_K \cdot \epsilon(\hat{Q}).$$

Let $\hat{Q}' = Q'|_{(v')^\perp}$. Then a similar computation as above yields

$$d(\hat{Q}') = d(\hat{Q}), \quad \epsilon(\hat{Q}') = \epsilon(\hat{Q}).$$

By induction on the rank, from the above we know that $v^\perp$ is isometric to $(v')^\perp$. It follows that (V, Q) is isometric to (V', Q'). □

To complete the classification over K, we need to determine which pairs

$$(d, \epsilon) \in K^\times/(K^\times)^2 \times \{\pm 1\}$$

can be realized as the invariants of a non-degenerate quadratic form of rank n.

Proposition 3.3.11. *Let K be a non-archimedean local field. Let $d \in K^\times/(K^\times)^2$ and $\epsilon \in \{\pm 1\}$.*

(1) *(d, ϵ) are the invariants of a rank 1 form if and only if $\epsilon = 1$.*
(2) *(d, ϵ) are the invariants of a rank 2 form if and only if $(d = -1 \Rightarrow \epsilon = 1)$.*
(3) *For any $n \geq 3$, (d, ϵ) are the invariants of a rank n form.*

Proof. (1) If Q is a rank 1 form, then $\epsilon(Q) = 1$ by definition. Conversely, for any $d \in K^\times/(K^\times)^2$, let $Q = dX^2$. Then $d(Q) = d$.

(2) If Q is a rank 2 form with $d(Q) = -1$, then writing $Q = aX^2 + bY^2$ we have $\epsilon(Q) = (a,b)_K = (a,-1/a)_K = (a,-a)_K = 1$. Conversely, if $d = -1$ and $\epsilon = 1$, then letting $Q = X^2 - Y^2$ we have $d(Q) = d, \epsilon(Q) = \epsilon$. If $d \neq -1$, then $K(\sqrt{-d})/K$ is a quadratic extension, so there exists $a' \in K^\times$ which is not a norm from $K(\sqrt{-d})$, i.e., $(a', -d)_K = -1$. Hence we can choose $a \in K^\times$ such that $(a,-d)_K = \epsilon$. Let $Q = aX^2 + adY^2$. Then $d(Q) = d$, and $\epsilon(Q) = (a, ad)_K = (a,-a)_K(a,-d)_K = \epsilon$.

(3) Let (d, ϵ) be arbitrary. Choose $a_3 \in K^\times$ such that $da_3 \neq -1 \in K^\times/(K^\times)^2$. Then by (2) there exists a rank 2 form $Q'(X_1, X_2)$ such that $d(Q') = da_3$ and $\epsilon(Q') = \epsilon \cdot (a_3, da_3)_K$. Let $Q = Q'(X_1, X_2) + a_3X_3^2 + \sum_{4 \leq i \leq n} X_i^2$. Then $d(Q) = d(Q')a_3 = d$, and

$$\epsilon(Q) = \epsilon(Q')(a_3, d(Q'))_K = \epsilon(Q')(a_3, da_3)_K = \epsilon.$$

□

For quadratic forms over $\mathbb{C}$ or $\mathbb{R}$, we define the Hasse invariant in the same way as the local non-archimedean case, using the Hilbert symbol over $\mathbb{C}$ or $\mathbb{R}$ (which is constantly 1 for $\mathbb{C}$). Over $\mathbb{R}$, if a quadratic form Q has signature (p, q), then clearly

$$d(Q) = (-1)^q, \quad \epsilon(Q) = (-1,-1)_{\mathbb{R}}^{\frac{q(q-1)}{2}} = (-1)^{\frac{q(q-1)}{2}}.$$

Thus we see that for $n = p + q \geq 4$, the pair $(d(Q), \epsilon(Q))$ does not uniquely determine q, and hence does not uniquely determine the equivalence class of Q of rank n. However, one easily checks Proposition 3.3.11 still holds for $K = \mathbb{R}$.

We now come to the classification of quadratic forms over a global field K (whose characteristic is not 2). In view of Theorem 3.3.1 and the classification over local fields, we only need to determine which families $(Q_v)_{v \in V_K}$, where Q_v is a non-degenerate quadratic form over K_v of rank n, are *globalizable*, in the sense that there exists a quadratic form Q over K such that $Q \sim Q_v$ over K_v for all v.

Theorem 3.3.12. *The family $(Q_v)_{v \in V_K}$ is globalizable if and only if the following conditions hold. Write $d_v := d(Q_v) \in K_v^\times/(K_v^\times)^2$ and $\epsilon_v := \epsilon(Q_v) \in \{\pm 1\}$.*

1. *There exists $d \in K^\times/(K^\times)^2$ mapping to $d_v \in K_v^\times$ for all v. (Note that the map $K^\times/(K^\times)^2 \to \prod_v K^\times/(K^\times)^2$ is injective by the local-global principle for being a square, so d is unique if it exists.)*
2. *We have $\epsilon_v = 1$ for almost all v, and $\prod_{v \in V_K} \epsilon_v = 1$.*

Lemma 3.3.13. *Let $b \in K^\times$. Let $T \subset V_K$ be a finite subset of even cardinality such that for all $v \in T$ we have $b \notin (K_v^\times)^2$. Then there exists $a \in K^\times$ such that $T = \{v \in V_K \mid (a,b)_{K_v} = -1\}$.*

Remark 3.3.14. By the product formula, clearly the assumptions on T are necessary.

Proof. If $T = \emptyset$ then we can take $a = 1$. Suppose $T \neq \emptyset$. Then $b \notin (K^\times)^2$, so $L = K(\sqrt{b})$ is a quadratic extension of K. Consider the Artin map $\psi = \psi_{L/K} : C_K \to \mathrm{Gal}(L/K) \cong \{\pm 1\}$. For $v \in T$, since b is not a square in K_v, the local extension L_w/K_v (for $w|v$) is non-trivial. Hence there exists $x_v \in K_v^\times$ that is not a norm from L_w. For $v \notin T$, we choose $x_v \in \mathrm{N}_{L_w/K_v}(L_w^\times)$, and we can choose x_v inside $\mathcal{O}_{K_v}^\times$ for almost all v. Then $x = (x_v) \in \mathbb{A}_K^\times$. We have

$$\psi(x) = \prod_v \psi_v(x_v) = \prod_{v \in T} (-1) = 1$$

since $|T|$ is even. Since $\ker \psi = \mathrm{N}_{L/K}(C_L)$, there exists $a \in K^\times$ such that $xa \in \mathrm{N}_{L/K}(\mathbb{A}_L^\times)$. Then for any v, we have $(a,b)_{K_v} = (x,b)_{K_v}$, and this is -1 if and only if $v \in T$ by the construction of x. □

Proof of Theorem 3.3.12. Necessity: If Q is a quadratic form over K such that $Q \sim Q_v$ over K_v for all v, then $d := d(Q) \in K^\times/(K^\times)^2$ maps to d_v. Write $Q = \sum_i a_i X_i^2$. Then $\epsilon_v = \prod_{i<j}(a_i, a_j)_{K_v}$. Condition (2) follows from the product formula for Hilbert symbols (Proposition 3.2.6).

Sufficiency. Let d and ϵ_v be as in (1) and (2). Let n be the common rank of Q_v. We shall construct a non-degenerate quadratic form Q over K of rank n such that $d(Q) = d$ and $\epsilon_v(Q) = \epsilon_v$ for all v. Here we denote by $\epsilon_v(Q)$ the Hasse invariant of Q viewed as a quadratic form over K_v. Then by the local classification we know that $Q \sim Q_v$ over K_v.

For $n = 1$, we can take $Q = dX^2$.

Suppose $n = 2$. Let $Q = aX^2 + adY^2$ with $a \in K^\times$ to be determined. Then $d(Q) = d$, and

$$\epsilon_v(Q) = (a, ad)_{K_v} = (a, -d)_{K_v}.$$

Let $T = \{v \in V_K \mid \epsilon_v = -1\}$. Then T is a finite even set by condition (2). For $v \in T$, we have $-d \notin (K_v^\times)^2$ since we have the local constraint $d_v = -1 \Rightarrow \epsilon_v = 1$ for the rank 2 form Q_v over K_v. Hence by Lemma 3.3.13, there exists $a \in K^\times$ such that $T = \{v \mid (a, -d)_{K_v} = 1\}$. Then the above discussion shows that $Q = aX^2 + adY^2$ satisfies the desired conditions.

Suppose $n = 3$. We shall construct $Q = Q_1(X_1, X_2) + a_3 X_3^2$ by constructing Q_1 and a_3. We have $d(Q) = d(Q_1)a_3$, so we want $d(Q_1)$ to be da_3. We have

$$\epsilon_v(Q) = \epsilon_v(Q_1)(a_3, d(Q_1))_{K_v},$$

so we want $\epsilon_v(Q_1)$ to be $\epsilon_v \cdot (a_3, d(Q_1))_{K_v}$, and in the presence of the previous condition this is the same as $\epsilon_v \cdot (a_3, da_3)_{K_v}$. Thus by the rank 2 case already proved, we only need to choose a_3 such that for each v, $(da_3, \epsilon_v \cdot (a_3, da_3)_{K_v})$ are the invariants of a rank 2 form over K_v, and such that $\epsilon_v \cdot (a_3, da_3)_{K_v} = 1$ for almost all v and $\prod_v \epsilon_v \cdot (a_3, da_3)_{K_v} = 1$. Only the first condition is not automatic. By Proposition 3.3.11, the condition is

$$da_3 \in (-1)(K_v^\times)^2 \Rightarrow \epsilon_v \cdot (a_3, da_3)_{K_v} = 1,$$

or equivalently

$$da_3 \in (-1)(K_v^\times)^2 \Rightarrow \epsilon_v \cdot (-d, -1)_{K_v} = 1.$$

Let $S = \{v \in V_K \mid (-d, -1)_{K_v} \neq \epsilon_v\}$. This is a finite set since for almost all v we have $(-d, -1)_{K_v} = \epsilon_v = 1$. By Weak Approximation (Lemma 3.1.12), there exists $a_3 \in K^\times$ such that for each $v \in S$ we have $da_3 \notin (-1)(K_v^\times)^2$ (since $-d^{-1}(K_v^\times)^2$ is a proper closed subset of $K_v^\times$, which follows from the fact that $(K_v^\times)^2$ is an open and hence closed subgroup). Then for any $v \in V_K$, we have

$$da_3 \in (-1)(K_v^\times)^2 \Rightarrow v \notin S \Rightarrow \epsilon_v \cdot (-d, -1)_{K_v} = 1.$$

For $n \geq 4$, we reduce to the construction of a form of rank $n-1$ by a similar argument and conclude by induction. (Since $n - 1 \geq 3$, we no longer have local constraints in the constructoin of a rank $n-1$ form, so the argument is easier.) □

References

[Art06] Emil Artin. *Algebraic numbers and algebraic functions*. AMS Chelsea Publishing, Providence, RI, 2006. Reprint of the 1967 original. 48

[AT09] Emil Artin and John Tate. *Class field theory*. AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original. 47, 53

[Bro94] Kenneth S. Brown. *Cohomology of groups*, volume 87 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. Corrected reprint of the 1982 original. 10, 22

[CF$^+$67] John William Scott Cassels, Albrecht Fröhlich, et al. Algebraic number theory: Proceedings of an instructional conference organized by the london mathematical society (a nato advanced study institute) with the support of the international mathematical union. 1967. 22, 24, 31, 44, 66

[Mil20] J.S. Milne. Class field theory (v4.03). pages 287+viii, 2020. Available at www.jmilne.org/math/. 24, 28, 66

[Neu13] Jürgen Neukirch. *Class field theory*. Springer, Heidelberg, 2013. The Bonn lectures, edited and with a foreword by Alexander Schmidt, Translated from the 1967 German original by F. Lemmermeyer and W. Snyder, Language editor: A. Rosenschon. 24, 26, 33

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. 22, 24, 28, 33

[Ser88] Jean-Pierre Serre. *Algebraic groups and class fields*, volume 117 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988. Translated from the French. 48

[Tat52] John Tate. The higher dimensional cohomology groups of class field theory. *Ann. of Math. (2)*, 56:294–297, 1952. 24

[Wei94] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994. 6